Unit A2

Number systems

Introduction

In this unit you will look at some different systems of numbers, and the rules for combining numbers in these systems. You have met many of these systems before, and you will study some of them in more detail later in the module.

For each number system, you will consider which numbers have additive and/or multiplicative inverses in the system. You will also look at when and how we can solve certain types of equations in the system, such as linear, quadratic and other polynomial equations. The answers to these questions provide insights into the structure of the various number systems, and this in turn enables us to define abstract structures like *fields* and *groups* which share some or all of the properties of number systems and arise in many areas of mathematics. You will meet fields in this unit, and study groups in Books B and E of this module.

1 Real numbers

In this section you will revise real numbers, and some important subsets of the real numbers. You will meet a collection of rules that the arithmetic of real numbers satisfies, and see that some subsets of the real numbers also satisfy these rules, whereas others do not. Finally, you will look at polynomial equations with real coefficients and consider the number of solutions they have.

1.1 Standard subsets of the real numbers

The set of all **real numbers** is denoted by $\mathbb{R}$. This set can be pictured as a number line, often called the **real line**. Each real number is represented by a point on the real line, and each point on this line represents a real number. Thus $\mathbb{R}$ is the set of all numbers that represent lengths along a line (and the negatives of such numbers). For example, the number $\frac{4}{3}$ corresponds to the point that lies a distance $\frac{4}{3}$ from 0 in the positive direction, as shown in Figure 1.

We sometimes refer to real numbers simply as *reals*.

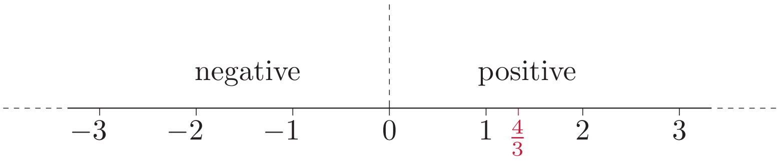


Figure 1 The real line showing the number $\frac{4}{3}$

The following standard subsets of the set $\mathbb{R}$ are used frequently in this module. You met some of them briefly in the previous unit.

The set $\mathbb{R}^*$ is the set of all non-zero real numbers. We can describe this set using set notation in various ways:

$$\mathbb{R}^* = \mathbb{R} - \{0\},$$
$$\mathbb{R}^* = (-\infty, 0) \cup (0, \infty),$$
$$\mathbb{R}^* = \{x \in \mathbb{R} : x \neq 0\}.$$

The set $\mathbb{Z}$ is the set of **integers**:

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

The set $\mathbb{N}$ is the set of positive integers, known as the **natural numbers**:

$$\mathbb{N} = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \ldots\}.$$

The set $\mathbb{Q}$ is the set of *rational numbers*. A **rational number** is a real number that can be expressed as a fraction whose numerator and denominator are integers. So we can describe $\mathbb{Q}$ using set notation as follows:

$$\mathbb{Q} = \{p/q : p \in \mathbb{Z}, q \in \mathbb{N}\}.$$

Notice that the sets $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ are related as follows:

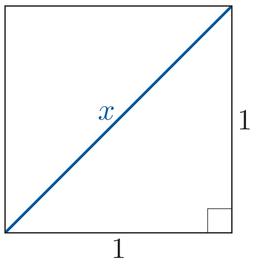
$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}.$$

That is, $\mathbb{N}$ is a subset of $\mathbb{Z}$, which in turn is a subset of $\mathbb{Q}$.

Rational numbers and irrational numbers

You have seen that $\mathbb{R}$ is the set of real numbers, and $\mathbb{Q}$ is the set of rational numbers, that is, the set of all numbers that can be expressed as fractions with integer numerators and denominators. The set $\mathbb{Q}$ is certainly a subset of the set $\mathbb{R}$, because each rational number represents a length along the real line (or the negative of such a length), in the way indicated at the beginning of this subsection. But it is not obvious at first sight whether $\mathbb{Q}$ is a *proper* subset of $\mathbb{R}$, or whether $\mathbb{Q}$ and $\mathbb{R}$ are in fact the same set. If it were possible to express every number that represents a length along the real line as a fraction with an integer numerator and denominator, then $\mathbb{Q}$ and $\mathbb{R}$ would be the same set.

In fact, as you will know, they are *not* the same set: some numbers that represent lengths cannot be expressed as fractions with integer numerators and denominators. This is a fact that was discovered by, and was surprising to, the ancient Greeks.



$x^2 = 1^2 + 1^2 = 2$

Figure 2 The diagonal of a square of side 1

For example, consider the length of the diagonal of a square of side 1, as shown in Figure 2. If this length is x then, by Pythagoras' Theorem, x must satisfy the equation $x^2 = 2$. However, there is no rational number that satisfies this equation.

To see this, suppose that there *is* such a number, say $x = p/q$, where p and q are positive integers and p/q is a fraction in lowest terms (so there is no integer greater than 1 that is a factor of both the numerator and denominator). Since $x = p/q$ satisfies the equation $x^2 = 2$, we know that

$$\frac{p^2}{q^2} = 2,$$

which gives $p^2 = 2q^2$, so p^2 is an even number. This tells us that p must also be an even number (because if p were odd, then p^2 would also be odd).

Now, since p is even, we can write $p = 2r$, where r is a positive integer, so $x = 2r/q$. Since x satisfies the equation $x^2 = 2$, we have

$$\frac{4r^2}{q^2} = 2,$$

which gives $q^2 = 2r^2$, so q^2 is an even number. In the same way as for p, this means that q must also be an even number.

But this is impossible: p and q cannot *both* be even, because then 2 would be a factor of both numerator and denominator and p/q is defined as being a fraction in lowest terms. It follows that there is no such rational number p/q. That is, there is no positive rational solution of the equation $x^2 = 2$, and since the negative solution of the equation is obtained simply by changing the sign of the positive solution, we have proved the following theorem.

Theorem A1

There is no rational number x such that $x^2 = 2$.

The proof that you have just seen is a classic example of a *proof by contradiction*. You will learn more about the technique of proof by contradiction, and other useful methods of proof, in the next unit, Unit A3, *Mathematical language and proof*.

So the set $\mathbb{Q}$ is definitely a *proper* subset of $\mathbb{R}$; that is, $\mathbb{R}$ contains numbers that are not in $\mathbb{Q}$. For example, $\mathbb{R}$ contains the number $\sqrt{2}$, which is the positive solution of the equation $x^2 = 2$; thus $\left(\sqrt{2}\right)^2 = 2$. The set $\mathbb{R}$ also contains many other numbers that are not rational numbers, such as $\sqrt{3}$, $\sqrt{7}$ and $\sqrt[3]{2}$ (where $\left(\sqrt[3]{2}\right)^3 = 2$), and so on. Indeed, it can be shown that, if m and n are natural numbers, and the equation $x^m = n$ has no integer solution, then the positive solution of this equation, written as $\sqrt[m]{n}$, cannot be rational.

Other real numbers that are not rational include the number π, which denotes the ratio of the circumference of a circle to its diameter, and the number e, the base for natural logarithms.

The real numbers that are not rational numbers are known as **irrational** numbers.

Johann Lambert

In 1767, in a paper read before the Berlin Academy of Sciences, the Swiss mathematician Johann Heinrich Lambert (1728–1777) provided the first proof that π is irrational. Lambert was a close friend of Leonhard Euler (1707–1783), who had invited him to Berlin in 1764, and of Joseph-Louis Lagrange (1736–1813) who was Euler's successor at the Berlin Academy after Euler returned to St Petersburg in 1766. In addition to this result on π, Lambert is well known for his work in geometry.

We often refer to rational and irrational numbers simply as *rationals* and *irrationals*, respectively.

Decimal expansions of rational numbers and irrational numbers

Every real number has a decimal expansion; for example,

$$\tfrac{1}{11} = 0.09\,09\,09\,09\ldots,$$
$$1\tfrac{1}{4} = 1.25,$$
$$\pi = 3.141\,592\,653\,589\ldots.$$

The decimal expansion of a *rational* number is always either a **terminating** (that is, finite) decimal, such as 1.25, or a **recurring** decimal, such as $0.09\,09\,09\,09\ldots$, in which the digits repeat in a regular pattern from some position onwards. The decimal representation of any rational number p/q can be obtained by using long division to divide q into p.

On the other hand, the decimal expansion of an *irrational* number is neither finite nor recurring. Instead, it continues for ever, with no pattern of digits that repeats indefinitely, such as π.

Every possible decimal number, finite or infinite, recurring or non-recurring, represents a real number.

1.2 Arithmetic of real numbers

Throughout your previous mathematical studies you will have used various rules of arithmetic whenever you carried out a calculation or an algebraic manipulation. For example, you will be familiar with the rule that the order in which you add or multiply two numbers does not affect the result, and with the rules for multiplying out brackets. Many of these rules of arithmetic come from the eleven simple properties of addition and multiplication of real numbers given in the box below.

Arithmetic in $\mathbb{R}$

Properties for addition

A1 Closure For all $a, b \in \mathbb{R}$,

$$a + b \in \mathbb{R}.$$

A2 Associativity For all $a, b, c \in \mathbb{R}$,

$$a + (b + c) = (a + b) + c.$$

A3 Additive identity For all $a \in \mathbb{R}$,

$$a + 0 = a = 0 + a.$$

A4 Additive inverses For each $a \in \mathbb{R}$, there is a number $-a \in \mathbb{R}$ such that

$$a + (-a) = 0 = (-a) + a.$$

A5 Commutativity For all $a, b \in \mathbb{R}$,

$$a + b = b + a.$$

Properties for multiplication

M1 Closure For all $a, b \in \mathbb{R}$,

$$a \times b \in \mathbb{R}.$$

M2 Associativity For all $a, b, c \in \mathbb{R}$,

$$a \times (b \times c) = (a \times b) \times c.$$

M3 Multiplicative identity For all $a \in \mathbb{R}$,

$$a \times 1 = a = 1 \times a.$$

M4 Multiplicative inverses For each $a \in \mathbb{R}^*$, there is a number $a^{-1} \in \mathbb{R}$ such that

$$a \times a^{-1} = 1 = a^{-1} \times a.$$

M5 Commutativity For all $a, b \in \mathbb{R}$,

$$a \times b = b \times a.$$

Property combining addition and multiplication

D1 Distributivity For all $a, b, c \in \mathbb{R}$,

$$a \times (b + c) = (a \times b) + (a \times c).$$

For clarity, the multiplication properties (M1 to M5) are shown in the above box using the symbol × but, as you will know, we often prefer to write simply ab for 'a multiplied by b', rather than $a \times b$.

The closure properties (A1 and M1) simply say that adding or multiplying two real numbers results in another real number.

The numbers 0 and 1 are known as the **additive identity** and **multiplicative identity** of $\mathbb{R}$, respectively. The number $-a$ in property A4 is known as the **additive inverse** or **negative** of a. The number a^{-1} in property M4 is known as the **multiplicative inverse** or **reciprocal** of a. One number, namely 0, does not have a multiplicative inverse, since there is no number that multiplies with 0 to make 1, and so 0 is excluded in the multiplicative inverses property (M4).

The set of rational numbers, $\mathbb{Q}$, also satisfies the eleven properties in the box above, in the sense that if $\mathbb{R}$ is replaced by $\mathbb{Q}$ throughout the box, then the properties are still true. (Of course, in property M4 the number 0 is excluded, just as for the real numbers.) You will see later that the same properties hold for the set of complex numbers, $\mathbb{C}$. However, if we restrict ourselves to the set of integers, $\mathbb{Z}$, then one of these properties is no longer true, as you are asked to show in the next exercise.

Exercise A57

(a) Show that $\mathbb{Z}$ does not satisfy the multiplicative inverses property (M4) by giving an example of an integer that does not have a multiplicative inverse.

(b) Which integers have a multiplicative inverse in $\mathbb{Z}$?

A set of numbers, with addition and multiplication defined in such a way that they satisfy the eleven properties in the box, together with a twelfth, rather trivial, property, namely that the additive and multiplicative identities are different numbers, is known as a **field**. (The twelfth property is included for technical reasons to ensure that the set $\{0\}$ with addition and multiplication is not a field; it need not concern you in this module.)

Thus a field is a number system that shares many of the properties of the arithmetic of the real numbers. You have seen that $\mathbb{R}$ and $\mathbb{Q}$ are fields, but that $\mathbb{Z}$ is not a field.

1.3 Solutions of polynomial equations

Even though the sets $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$, with addition and multiplication, are all fields and hence share similar rules of arithmetic, they are quite different in other ways.

Some of their differences are highlighted by considering which polynomial equations, with coefficients in the set in question, have a solution in that set. Here is a reminder of what we mean by a polynomial equation and its coefficients.

Definitions

A **polynomial** in x of **degree** n is an expression of the form

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_n$ are numbers, called the **coefficients** of the polynomial, with $a_n \neq 0$.

A **polynomial equation** in x of degree n is an equation of the form $p(x) = 0$, where $p(x)$ is a polynomial in x of degree n.

Polynomial equations (and polynomials) of degrees 1, 2 and 3 are called **linear**, **quadratic** and **cubic**, respectively.

So, for example, the following are polynomials:

$$\tfrac{1}{2}x^3 - x^2 + \sqrt{3}, \quad 2x - 7, \quad x^2 - 2,$$

and the following are polynomial equations:

$$\tfrac{1}{2}x^3 - x^2 + \sqrt{3} = 0, \quad 2x - 7 = 0, \quad x^2 = 2.$$

(The third equation here is a rearrangement of $x^2 - 2 = 0$.)

The equation $x^2 = 2$ is a polynomial equation with coefficients in $\mathbb{Q}$, and you saw earlier in this section that this equation has no solution in $\mathbb{Q}$. However, the equation $x^2 = 2$ can also be considered as an equation with coefficients in $\mathbb{R}$, and it does have solutions in $\mathbb{R}$, namely the two solutions $\pm\sqrt{2}$. In this sense, $\mathbb{R}$ seems a ‘better’ number system than $\mathbb{Q}$.

In the next exercise, you are asked to look at some *linear* equations, and consider whether they have solutions in the sets $\mathbb{Q}$ and $\mathbb{R}$.

Exercise A58

(a) The following linear equations have coefficients in $\mathbb{Q}$. Determine whether each of them has a solution in $\mathbb{Q}$.

(i) $5x + 10 = 0$ (ii) $5x + 1 = 0$

(b) The following linear equations have coefficients in $\mathbb{R}$. Determine whether each of them has a solution in $\mathbb{R}$.

(i) $2x - 6 = 0$ (ii) $\sqrt{3}x + 7 = 0$

In fact, every linear equation with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{Q}$, because the equation $ax + b = 0$ where $a, b \in \mathbb{Q}$ and $a \neq 0$ has exactly one solution, namely $x = -b/a$, which is rational. (Here we have used properties A2–A4 and M1–M5 to deduce that $x = -ba^{-1} \in \mathbb{Q}$, although we usually express this using ‘division’ as $x = -b/a \in \mathbb{Q}$.) Similarly, every linear equation with coefficients in $\mathbb{R}$ has exactly one solution in $\mathbb{R}$.

Let us now look at quadratic equations. The example of the quadratic equation $x^2 = 2$ has already shown you that not every quadratic equation with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{Q}$. In the next exercise, you are asked to look at some quadratic equations with coefficients in $\mathbb{R}$, and consider whether they have solutions in $\mathbb{R}$.

Remember that it is usually best to solve a quadratic equation by *factorisation* if you can. Otherwise, you can use the **quadratic formula**, which tells you that the solutions of the quadratic equation $ax^2 + bx + c = 0$, where $a, b, c \in \mathbb{R}$ and $a \neq 0$, are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Exercise A59

Solve the following quadratic equations, stating how many solutions each equation has in $\mathbb{R}$.

(a) $x^2 - 7x + 12 = 0$ (b) $x^2 + 6x + 9 = 0$ (c) $2x^2 + 5x - 3 = 0$

(d) $2x^2 - 2x - 1 = 0$ (e) $x^2 - 2x + 5 = 0$ (f) $x^2 - 2\sqrt{3}x + 3 = 0$

Exercise A59 illustrates that some quadratic equations with coefficients in $\mathbb{R}$ have two solutions in $\mathbb{R}$, some have only one and some have none. In either of the first two cases, the solutions may be rational or irrational. Although you may be accustomed to equations with integer coefficients such as those in Exercise A59(a)–(e), these facts still apply if some or all of the coefficients are irrational; that is, if the coefficients are any real numbers.

So, although the set $\mathbb{R}$ seems ‘better’ than the set $\mathbb{Q}$, working with $\mathbb{R}$ still does not enable us to find solutions of *all* quadratic equations. In Section 2 you will see that working with the set of complex numbers, $\mathbb{C}$, *does* enable us to find solutions of *all* quadratic equations, and in fact it enables us to find solutions of all polynomial equations.

1.4 The Factor Theorem

In the previous subsection we looked at the issue of whether polynomial equations with coefficients in $\mathbb{Q}$ or in $\mathbb{R}$ have solutions in $\mathbb{Q}$ or in $\mathbb{R}$, respectively. We now confine our attention to polynomial equations with coefficients in $\mathbb{R}$, and consider the maximum number of solutions that such an equation of degree n can have. For example, you already know that a linear equation (that is, a polynomial equation of degree 1) has exactly one solution, and a quadratic equation (that is, a polynomial equation of degree 2) has a maximum of two solutions. We also look at ways in which we can sometimes find some or all of the solutions of a polynomial equation.

We will mainly discuss these issues in terms of polynomials, rather than polynomial equations. We make the following definition.

Definition

The **roots** (or **zeros**) of a polynomial $p(x)$ are the solutions of the equation $p(x) = 0$.

So finding the roots of a polynomial $p(x)$ means the same as finding the solutions of the polynomial equation $p(x) = 0$.

A polynomial with coefficients in $\mathbb{R}$ is called a **real polynomial**.

You know that you can often find the roots of a quadratic polynomial by *factorising* it. Factorisation can also be useful for higher-degree polynomials. In general, if a polynomial $p(x)$ can be expressed in the form

$$p(x) = s(x)t(x),$$

where $s(x)$ and $t(x)$ are polynomials whose degree is less than that of $p(x)$, then we say that $s(x)$ and $t(x)$ are **factors** of $p(x)$.

The following theorem can help us to factorise polynomials. You will see a proof of this theorem in Unit A3.

Theorem A2 Factor Theorem (in $\mathbb{R}$)

Let $p(x)$ be a real polynomial, and let $\alpha \in \mathbb{R}$. Then $p(\alpha) = 0$ if and only if $x - \alpha$ is a factor of $p(x)$.

The phrase ‘if and only if’ is a means of stating two *converse* mathematical statements at once; here it tells us that the following two statements are both true:

- If $p(\alpha) = 0$, then $x - \alpha$ is a factor of $p(x)$.
- If $x - \alpha$ is a factor of $p(x)$, then $p(\alpha) = 0$.

You will revise the use of the phrase ‘if and only if’ in more detail in Unit A3.

The following worked exercise demonstrates how you can use the Factor Theorem. It also demonstrates how, once you know that a particular polynomial $p(x)$ has a factorisation of the form $p(x) = (x - \alpha)q(x)$, where you know the value of the root α, you can find the polynomial $q(x)$ by **equating corresponding coefficients**, also known as *comparing coefficients*.

Worked Exercise A24

Show that $x - 2$ is a factor of the cubic polynomial

$$p(x) = x^3 + x^2 - x - 10,$$

and find the corresponding factorisation of $p(x)$.

Solution

Evaluate $p(2)$ and apply the Factor Theorem.

We have

$$p(2) = 2^3 + 2^2 - 2 - 10 = 8 + 4 - 2 - 10 = 0.$$

So, by the Factor Theorem (Theorem A2), $p(x)$ has the factor $x - 2$.

So, since $p(x)$ is a cubic polynomial, it must be the product of $x - 2$ and a quadratic polynomial.

Hence

$$x^3 + x^2 - x - 10 = (x - 2)(ax^2 + bx + c),$$

for some real numbers a, b and c.

To find the coefficients a, b and c of the quadratic polynomial, compare coefficients on each side of the equation. Start with the coefficients of the highest-degree terms and the constant terms.

Equating the coefficients of x^3 gives $1 = a$. Equating the constant terms gives $-10 = -2c$, so $c = 5$. Thus we have

$$x^3 + x^2 - x - 10 = (x - 2)(x^2 + bx + 5).$$

We can compare the coefficients of x^2 or x; we choose x^2.

Equating the coefficients of x^2 gives $1 = -2 + b$, so $b = 3$. Hence

$$x^3 + x^2 - x - 10 = (x - 2)(x^2 + 3x + 5).$$

We can equate the coefficients of x to check our answer. This gives $-1 = 5 - 2b$, so again $b = 3$, as expected.

Exercise A60

(a) For what value of k is $x+3$ a factor of

$$p(x) = x^3 + kx^2 + 6x + 36\,?$$

(b) For this value of k, find the corresponding factorisation of $p(x)$.

The following theorem can be proved by repeatedly applying the Factor Theorem, as you will see in Unit A3.

Theorem A3

Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a real polynomial, and suppose that $p(x)$ has n distinct real roots $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then

$$p(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

For example, the polynomial

$$p(x) = 2x^4 - 8x^3 - 2x^2 + 32x - 24$$

has the four distinct real roots 1, 2, 3 and -2, as you can check by evaluating $p(1)$, $p(2)$, $p(3)$ and $p(-2)$, and so (from Theorem A3)

$$p(x) = 2(x-1)(x-2)(x-3)(x+2).$$

In fact, as you will see in Subsection 2.4, *every* real polynomial $p(x)$ of degree n has a factorisation of the form given in Theorem A3, although the roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ need not be distinct and may include non-real *complex numbers*. We have the following.

A real polynomial of degree n has at most n distinct roots (some of which may be complex numbers).

We now look at ways in which you can sometimes find some or all of the roots of a real polynomial.

The following useful observation should be familiar from your previous studies of factorising quadratics. If you multiply out the brackets

$$(x-\alpha)(x-\beta),$$

where α and β are real numbers, then you obtain a quadratic polynomial $p(x) = x^2 + bx + c$ such that

- the value of c, the constant term, is $\alpha\beta$;
- the value of b, the coefficient of x, is $-(\alpha+\beta)$.

We can make a similar observation about the result of multiplying out the n brackets

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

When we multiply out these brackets, we obtain a polynomial of degree n such that the coefficient of x^n is 1. This polynomial has the following properties.

Suppose that

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are real numbers. Then

- $a_0 = (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n$;
- $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$.

For example,

$$x^3 + x^2 - 5x + 3 = (x - 1)(x - 1)(x + 3),$$

so $a_0 = 3$, $\alpha_1 = 1$, $\alpha_2 = 1$, $\alpha_3 = -3$ and $a_{n-1} = 1$ and we have

$$3 = (-1)^3 \times 1 \times 1 \times (-3)$$

and

$$1 = -(1 + 1 - 3).$$

The expression for the constant term a_0 in the box above is obtained by comparing constant terms on each side of the equation at the top of the box.

Similarly, the expression for the coefficient a_{n-1} is obtained by equating the corresponding coefficients of x^{n-1}, as follows. When the brackets on the right-hand side are multiplied out, each term in x^{n-1} arises by choosing the variable x from $n - 1$ of the brackets, and the constant term from the remaining bracket. Choosing the constant term from the first bracket gives $-\alpha_1 x^{n-1}$, choosing the constant term from the second bracket gives $-\alpha_2 x^{n-1}$, and so on. Adding all these terms and comparing the resulting total coefficient with the coefficient of x^{n-1} on the left-hand side gives $a_{n-1} = -(\alpha_1 + \alpha_2 + \cdots + \alpha_n)$.

The observations in the box above can help us factorise a polynomial if we know that all of its roots are integers.

Worked Exercise A25

Given that all the roots of the polynomial

$$p(x) = x^3 - 6x^2 - 9x + 14$$

are integers, write $p(x)$ as a product of linear factors.

Solution

By the first property above, all the roots are factors of 14.

Since all the roots of $p(x)$ are integers, the only possible roots are the factors of 14, that is, ± 1, ± 2, ± 7, ± 14. Considering these in turn, we obtain the following table.

x	1	-1	2	-2	7	-7	14	-14
$p(x)$	0	16	-20	0	0	-560	1456	-3780

The only roots of $p(x)$ are $x = 1$, $x = -2$ and $x = 7$.

Actually, since we know that a cubic polynomial has at most only three roots, we do not need to complete the table once we have found three!

Also, the coefficient of the highest power of x in $p(x)$ is 1. Hence (by Theorem A3)

$$p(x) = (x - 1)(x + 2)(x - 7).$$

As a check, we note that the coefficient of x^2 is equal to minus the sum of the roots, $-6 = -(1 - 2 + 7)$.

Exercise A61

(a) Given that all the roots of the polynomial

$$p(x) = x^3 - 9x^2 + 23x - 15$$

are integers, write $p(x)$ as a product of linear factors.

(b) Given that all the solutions are integers, solve the equation

$$x^3 - 3x^2 + 4 = 0.$$

Use the property relating the sum of the roots to the coefficient of x^2 to write the equation as a product of linear factors.

Exercise A62

(a) Determine a polynomial equation whose solutions are $1, 2, 3, -3$.

(b) Determine a cubic equation whose only solutions are 2 and 3.

2 Complex numbers

In this section you will revise complex numbers and their properties. You will see how to find complex roots of certain polynomial equations, and how the complex exponential function can be used to represent complex numbers.

2.1 What is a complex number?

Earlier you saw that the real numbers correspond to points on the real line. In this subsection you will see that the *complex numbers* correspond to points in the plane.

Complex numbers arise naturally as solutions of quadratic equations. You have seen that some quadratic equations have no solutions in $\mathbb{R}$, that is, no real solutions. For example, you saw in Exercise A59(e) that the equation $x^2 - 2x + 5 = 0$ has no real solutions, because there is no real number whose square is -16. We can extend the set of real numbers to ensure that every quadratic equation has at least one solution.

To do this, we introduce a new number, denoted by i, which is defined to have the property that $i^2 = -1$. We assume that i combines with itself, and with real numbers, according to the usual rules of arithmetic. In particular, we assume that if we multiply i by any real number y then we obtain the product $iy = yi$, and if we then add this product to any real number x we obtain the sum $x + iy = x + yi$. Sums of this form are known as *complex numbers*, and they are the numbers we need to enable us to find solutions of every quadratic equation.

Definitions

A **complex number** is an expression of the form $x + iy$, where x and y are real numbers and $i^2 = -1$. The set of all complex numbers is denoted by $\mathbb{C}$.

A complex number $z = x + iy$ has **real part** x and **imaginary part** y; we write

$$\operatorname{Re} z = x \quad \text{and} \quad \operatorname{Im} z = y.$$

Two complex numbers are equal when their real parts *and* their imaginary parts are equal.

Remarks

1. Any real number x can be written in the form $x + i0$, and any complex number of the form $x + i0$ is usually written simply as x. In this sense, $\mathbb{R}$ is a subset of $\mathbb{C}$. The complex number $0 + i0$ is written as 0.
2. We follow the usual practice of writing a general complex number as $x + iy$, but a particular complex number as, for example, $2 + 3i$, rather than $2 + i3$.

   We also write $2 - 3i$ rather than $2 + (-3)i$, and we write $2 + i\sqrt{3}$ rather than $2 + \sqrt{3}i$, to avoid confusion with $2 + \sqrt{3i}$ (where the number i is included under the square root).
3. Note that $\operatorname{Re} z$ and $\operatorname{Im} z$ are both real numbers. For example, if $z = 2 - 3i$, then $\operatorname{Re} z = 2$ and $\operatorname{Im} z = -3$.
4. A complex number of the form $0 + iy$ (where $y \neq 0$) is sometimes called an **imaginary number**.

You know that every positive real number has two square roots. When you are working with the complex numbers, every negative real number also has two square roots, as follows.

Square roots of a negative real number

For a positive real number d, the square roots of $-d$ are $\pm i\sqrt{d}$.

You can check that $\pm i\sqrt{d}$ are square roots of $-d$ by using the usual rules of arithmetic:

$$\left(\pm i\sqrt{d}\right)^2 = i^2\left(\sqrt{d}\right)^2 = (-1) \times d = -d.$$

You will see in Subsection 2.4 why these are the *only* square roots of $-d$.

We can solve quadratic equations that have no real solutions by using the fact in the box above, together with the quadratic formula. When we apply this formula to a quadratic equation that has no real solutions, we obtain a term in the numerator of the form $\pm\sqrt{-d}$, where d is a positive number. In real terms, this is meaningless, because the square root sign applies only to positive real numbers, or zero. However, when we are working with complex numbers, we can take this term to mean the two square roots of $-d$, which are as given in the box above. This is illustrated in the worked exercise below.

The equation in this worked exercise is the one from Exercise A59(e), rewritten using z as the variable name. We often use the letter z for a **complex variable** (a variable that represents a complex number).

Worked Exercise A26

Solve the quadratic equation

$$z^2 - 2z + 5 = 0.$$

Solution

The quadratic formula gives

$$z = \frac{2 \pm \sqrt{-16}}{2} = \frac{2 \pm i\sqrt{16}}{2} = \frac{2 \pm 4i}{2} = 1 \pm 2i.$$

We can check that the two complex numbers found in Worked Exercise A26 satisfy the equation we were trying to solve. We use the usual rules of arithmetic, and substitute -1 for i^2 wherever it appears.

For example, if $z = 1 + 2i$, then

$$\begin{aligned} z^2 - 2z + 5 &= (1+2i)^2 - 2(1+2i) + 5 \\ &= 1 + 4i + 4i^2 - 2 - 4i + 5 \\ &= 1 + 4i + 4(-1) - 2 - 4i + 5 \\ &= 1 + 4i - 4 - 2 - 4i + 5 \\ &= 0. \end{aligned}$$

The solution $z = 1 - 2i$ can be checked in the same way.

Similarly, it can be checked that the method of Worked Exercise A26 will in general give us two complex numbers that satisfy the quadratic equation we are trying to solve. So the use of the number i enables us to find solutions of any quadratic equation. You will see later in this section that the use of i ensures that *all* polynomial equations have solutions, even those whose coefficients are themselves complex numbers. This, in turn, means that *any* polynomial can be factorised into a product of linear factors; for example,

$$\begin{aligned} z^2 - 2z + 5 &= (z - (1+2i))(z - (1-2i)) \\ &= (z - 1 - 2i)(z - 1 + 2i). \end{aligned}$$

Exercise A63

Solve the following equations, giving all solutions in $\mathbb{C}$.

(a) $z^2 - 4z + 7 = 0$

(b) $z^2 - iz + 2 = 0$

(c) $z^3 - 3z^2 + 4z - 2 = 0$ (*Hint*: $z = 1$ is one solution.)

(d) $z^4 - 16 = 0$

The complex plane

Just as there is a one-to-one correspondence between the real numbers and the points on the real line, so there is a one-to-one correspondence between the complex numbers and the points in the plane. This correspondence is given by

$$\begin{aligned} f\colon \mathbb{C} &\longrightarrow \mathbb{R}^2 \\ x+iy &\longmapsto (x,y). \end{aligned}$$

Thus we can represent points in the plane by complex numbers and, conversely, we can represent complex numbers by points in the plane. When we do this, we refer to the plane as the **complex plane**, and we often refer to the complex numbers as *points* in the complex plane. A diagram, such as Figure 3, showing complex numbers represented as points in the plane in this way is sometimes called an **Argand diagram**.

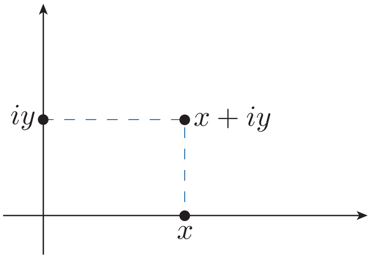


Figure 3 The complex plane

The first widely recognised publication of this idea appeared in a manuscript *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques* dated 1806 by a mathematician described only as Monsieur Argand. Until recently he was believed to be Jean-Robert Argand but further research by Gert Schubring (2001), first presented in 1998, has shown that this is a misattribution and his first name is unknown.

(Source: Schubring, G. (2001) 'Argand and the early work on graphical representation: New sources and interpretations', *Proceedings of the Wessel Symposium at the Royal Danish Academy of Sciences and Letters*. Copenhagen, August 11–15 1998, pp. 125–146.)

Real numbers are represented in the complex plane by points on the horizontal axis; this axis is called the **real axis**. Similarly, numbers of the form iy are represented by points on the vertical axis; this axis is called the **imaginary axis**.

Exercise A64

Draw a diagram showing each of the following points in the complex plane:

$$2+3i, \quad -3+2i, \quad -2-i, \quad 3-2i.$$

2.2 Arithmetic of complex numbers

Arithmetic operations on complex numbers are carried out as for real numbers, except that we replace i^2 by -1 wherever it occurs.

Worked Exercise A27

Let $z_1 = 1 + 2i$ and $z_2 = 3 - 4i$. Determine the following complex numbers.

(a) $z_1 + z_2$ (b) $z_1 - z_2$ (c) $z_1 z_2$ (d) z_1^2

Solution

The usual rules of arithmetic apply, with the additional property that $i^2 = -1$.

(a)
$$\begin{aligned} z_1 + z_2 &= (1 + 2i) + (3 - 4i) \\ &= (1 + 3) + (2 - 4)i \\ &= 4 - 2i \end{aligned}$$

(b)
$$\begin{aligned} z_1 - z_2 &= (1 + 2i) - (3 - 4i) \\ &= (1 - 3) + (2 + 4)i \\ &= -2 + 6i \end{aligned}$$

(c)
$$\begin{aligned} z_1 z_2 &= (1 + 2i)(3 - 4i) \\ &= 3 + 6i - 4i - 8i^2 \\ &= 3 + 2i + 8 \\ &= 11 + 2i \end{aligned}$$

(d)
$$\begin{aligned} z_1^2 &= (1 + 2i)(1 + 2i) \\ &= 1 + 2i + 2i + 4i^2 \\ &= 1 + 4i - 4 \\ &= -3 + 4i \end{aligned}$$

Worked Exercise A27 illustrates how we add, subtract and multiply two given complex numbers. We can apply the same methods to two general complex numbers $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, and obtain the following formal definitions of addition, subtraction and multiplication in $\mathbb{C}$.

Definitions

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$ be any complex numbers. Then the following operations can be applied.

Addition $z_1 + z_2 = (x_1 + x_2) + i(y_1 + y_2)$

Subtraction $z_1 - z_2 = (x_1 - x_2) + i(y_1 - y_2)$

Multiplication $z_1 z_2 = (x_1 x_2 - y_1 y_2) + i(x_2 y_1 + x_1 y_2)$

There is no need to remember or look up these formulas. For calculations, you can use the methods of Worked Exercise A27. Note that, since the usual rules of algebra hold, so do familiar algebraic identities such as

$$(z_1 + z_2)^2 = z_1^2 + 2z_1z_2 + z_2^2$$

and

$$z_1^2 - z_2^2 = (z_1 - z_2)(z_1 + z_2).$$

An obvious omission from the list of definitions in the box above is *division*. We will return to division after looking at the *complex conjugate* and *modulus* of a complex number.

Exercise A65

Determine the following complex numbers.

(a) $(3 - 5i) + (2 + 4i)$ (b) $(2 - 3i)(-3 + 2i)$ (c) $(5 + 3i)^2$

(d) $(1 + i)(7 + 2i)(4 - i)$

Complex conjugate

Many manipulations involving complex numbers, such as division, can be simplified by using the idea of a *complex conjugate*.

Definition

The **complex conjugate** $\overline{z}$ of the complex number $z = x + iy$ is the complex number $x - iy$.

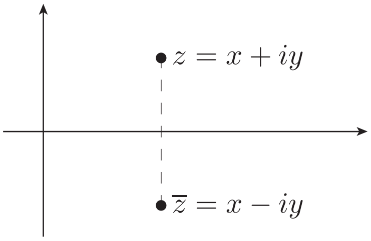


Figure 4 The complex conjugate

For example, if $z = 1 - 2i$, then $\overline{z} = 1 + 2i$. In geometric terms, $\overline{z}$ is the image of z under reflection in the real axis, as shown in Figure 4.

Exercise A66

Let $z_1 = -2 + 3i$ and $z_2 = 3 - i$. Write down $\overline{z_1}$ and $\overline{z_2}$, and draw a diagram showing z_1, z_2, $\overline{z_1}$ and $\overline{z_2}$ in the complex plane.

The following properties of complex conjugates are particularly useful.

Properties of complex conjugates

Let z_1, z_2 and z be any complex numbers. Then:

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$
2. $\overline{z_1 z_2} = \overline{z_1} \times \overline{z_2}$
3. $z + \overline{z} = 2\,\mathrm{Re}\,z$
4. $z - \overline{z} = 2i\,\mathrm{Im}\,z$.

To prove that property 1 holds, we consider two arbitrary complex numbers. Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then

$$\begin{aligned}\overline{z_1 + z_2} &= \overline{(x_1 + x_2) + i(y_1 + y_2)}\\ &= (x_1 + x_2) - i(y_1 + y_2)\\ &= (x_1 - iy_1) + (x_2 - iy_2)\\ &= \overline{z_1} + \overline{z_2}.\end{aligned}$$

Exercise A67

Use a similar approach to prove that properties 2, 3 and 4 all hold.

Modulus of a complex number

We also need the idea of the *modulus* of a complex number. Recall that the modulus of a real number x is defined by

$$|x| = \begin{cases} x, & \text{if } x \geq 0,\\ -x, & \text{if } x < 0.\end{cases}$$

For example, $|7| = 7$ and $|-6| = 6$.

In other words, $|x|$ is the distance from the point x on the real line to the origin. We extend this definition to complex numbers, as illustrated in Figure 5.

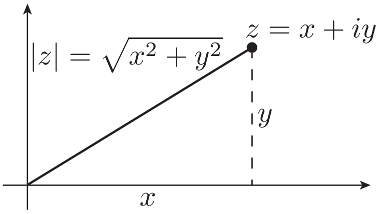


Figure 5 The modulus of a complex number

Definition

The **modulus** $|z|$ of a complex number z is the distance from the point z in the complex plane to the origin.

Thus the modulus of the complex number $z = x + iy$ is

$$|z| = \sqrt{x^2 + y^2}.$$

For example, if $z = 3 - 4i$, then $|z| = \sqrt{3^2 + (-4)^2} = \sqrt{25} = 5$.

Exercise A68

Determine the modulus of each of the following complex numbers.

(a) $5 + 12i$ (b) $1 + i$ (c) -5

The modulus of a complex number has many properties similar to those of the modulus of a real number.

Properties of the modulus

1. $|z| \geq 0$ for any $z \in \mathbb{C}$, with equality only when $z = 0$.
2. $|z_1 z_2| = |z_1|\,|z_2|$ for any $z_1, z_2 \in \mathbb{C}$.

Property 1 is clear from the definition of $|z|$. Property 2 can be shown to hold in a similar way to property 2 of complex conjugates in the solution to Exercise A67.

The following useful result shows the link between modulus and distance in the complex plane.

Distance formula for $\mathbb{C}$

The distance between the points z_1 and z_2 in the complex plane is $|z_1 - z_2|$.

This is obtained by applying Pythagoras' Theorem to the triangle shown in Figure 6. The formula holds wherever the points z_1 and z_2 are situated in the complex plane.

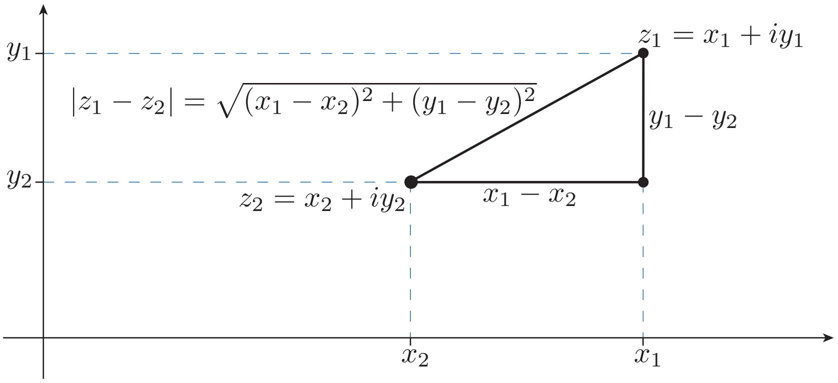


Figure 6 The distance formula for $\mathbb{C}$

Exercise A69

For each of the following pairs z_1, z_2 of complex numbers, draw a diagram showing z_1 and z_2 in the complex plane, find $z_1 - z_2$ and evaluate $|z_1 - z_2|$.

(a) $z_1 = 3 + i, \quad z_2 = 1 + 2i.$

(b) $z_1 = 1, \quad z_2 = i.$

(c) $z_1 = -5 - 3i, \quad z_2 = 2 - 7i.$

The following properties describe the relationship between the modulus and the complex conjugate of a complex number.

Conjugate–modulus properties

1. $|\overline{z}| = |z|$ for all $z \in \mathbb{C}$.
2. $z\overline{z} = |z|^2$ for all $z \in \mathbb{C}$.

To see why these properties hold, let $z = x + iy$. Then $\overline{z} = x - iy = x + i(-y)$, so

$$|\overline{z}| = \sqrt{x^2 + (-y)^2} = \sqrt{x^2 + y^2} = |z|.$$

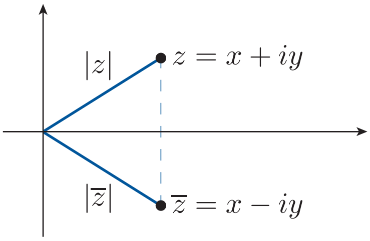


Figure 7 The complex conjugate

This can also be seen geometrically in Figure 7, where the distances from the origin to both z and its complex conjugate $\overline{z}$ are the same. We also have

$$z\overline{z} = (x + iy)(x - iy) = x^2 + ixy - ixy - i^2y^2 = x^2 + y^2 = |z|^2.$$

Division of complex numbers

The second of the conjugate–modulus properties in the above box enables us to find reciprocals of complex numbers and to divide one complex number by another, as shown in the next worked exercise. In exactly the same way as for real numbers, we cannot find a reciprocal of zero, nor divide any complex number by zero.

Worked Exercise A28

(a) Find the reciprocal of $2 - 5i$.

(b) Find the quotient $\dfrac{3 - i}{1 + 2i}$.

Solution

(a) To express the reciprocal $1/(2-5i)$ in the form $a+ib$, we multiply the numerator and denominator by $2+5i$, the complex conjugate of the denominator $2-5i$, and then use the second conjugate–modulus property.

The reciprocal is

$$\begin{aligned}\frac{1}{2-5i} &= \frac{1(2+5i)}{(2-5i)(2+5i)}\\ &= \frac{2+5i}{|2-5i|^2}\\ &= \frac{2+5i}{4+25}\\ &= \tfrac{2}{29}+\tfrac{5}{29}i = \tfrac{1}{29}(2+5i)\,.\end{aligned}$$

(b) We multiply the numerator and denominator by $1-2i$, the complex conjugate of the denominator $1+2i$, and then use the second conjugate–modulus property.

$$\begin{aligned}\frac{3-i}{1+2i} &= \frac{(3-i)(1-2i)}{(1+2i)(1-2i)}\\ &= \frac{3-i-6i+2i^2}{|1+2i|^2}\\ &= \frac{1-7i}{1+4}\\ &= \tfrac{1}{5}-\tfrac{7}{5}i = \tfrac{1}{5}(1-7i)\,.\end{aligned}$$

The method used in Worked Exercise A28, of multiplying the numerator and denominator by the complex conjugate of the denominator, enables us to find the reciprocal of any non-zero complex number z, and the quotient z_1/z_2 of any two complex numbers z_1 and z_2, where $z_2 \neq 0$. We can obtain general formulas as follows.

For the reciprocal, we have

$$\frac{1}{z} = \frac{1\times\overline{z}}{z\times\overline{z}} = \frac{\overline{z}}{|z|^2}, \quad \text{for } z \neq 0.$$

If $z = x+iy$, then $\overline{z} = x-iy$ and $|z|^2 = x^2+y^2$, so we obtain

$$\frac{1}{x+iy} = \frac{x-iy}{x^2+y^2}.$$

For the quotient z_1/z_2, we have

$$\frac{z_1}{z_2} = \frac{z_1\times\overline{z_2}}{z_2\times\overline{z_2}} = \frac{z_1\overline{z_2}}{|z_2|^2}, \quad \text{for } z_2 \neq 0.$$

If $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$, this can be rewritten as

$$\frac{x_1 + iy_1}{x_2 + iy_2} = \frac{(x_1 + iy_1)(x_2 - iy_2)}{x_2^2 + y_2^2} = \frac{(x_1x_2 + y_1y_2) + i(x_2y_1 - x_1y_2)}{x_2^2 + y_2^2}.$$

These formulas may be used in theoretical work, but for calculations of reciprocals and quotients it is simpler to use the method of Worked Exercise A28.

Exercise A70

Find the reciprocal of each of the following complex numbers.

(a) $3 - i$ (b) $-1 + 2i$

Exercise A71

Evaluate each of the following quotients.

(a) $\dfrac{5}{2 - i}$ (b) $\dfrac{2 + 3i}{-3 + 4i}$

Arithmetic properties of complex numbers

The set of complex numbers $\mathbb{C}$ satisfies the eleven properties previously given for arithmetic in $\mathbb{R}$. These properties are stated in the box below (their proofs are not given here). Since $\mathbb{C}$ satisfies these eleven properties (and also satisfies the twelfth, trivial, property mentioned in Subsection 1.2), it is a *field*, like $\mathbb{R}$ and $\mathbb{Q}$.

Arithmetic in $\mathbb{C}$

Properties for addition

A1 Closure For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 + z_2 \in \mathbb{C}.$$

A2 Associativity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3.$$

A3 Additive identity For all $z \in \mathbb{C}$,

$$z + 0 = z = 0 + z.$$

A4 Additive inverses For each $z \in \mathbb{C}$, there is a number $-z \in \mathbb{C}$ such that

$$z + (-z) = 0 = (-z) + z.$$

A5 Commutativity For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 + z_2 = z_2 + z_1.$$

Properties for multiplication

M1 Closure For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 \times z_2 \in \mathbb{C}.$$

M2 Associativity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \times (z_2 \times z_3) = (z_1 \times z_2) \times z_3.$$

M3 Multiplicative identity For all $z \in \mathbb{C}$,

$$z \times 1 = z = 1 \times z.$$

M4 Multiplicative inverses For each $z \in \mathbb{C} - \{0\}$, there is a number $z^{-1} \in \mathbb{C}$ such that

$$z \times z^{-1} = 1 = z^{-1} \times z.$$

M5 Commutativity For all $z_1, z_2 \in \mathbb{C}$,

$$z_1 \times z_2 = z_2 \times z_1.$$

Property combining addition and multiplication

D1 Distributivity For all $z_1, z_2, z_3 \in \mathbb{C}$,

$$z_1 \times (z_2 + z_3) = (z_1 \times z_2) + (z_1 \times z_3).$$

In particular, $0 = 0 + 0i$ plays the same role in $\mathbb{C}$ as the real number 0 does in $\mathbb{R}$: it is the **additive identity**. The number $1 = 1 + 0i$ plays the same role as 1: it is the **multiplicative identity**. We also have that the **additive inverse** (or negative) of $z = x + iy$ is $-z = -x - iy$, and the **multiplicative inverse** (or reciprocal) of $z = x + iy$ is

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} = \frac{x - iy}{x^2 + y^2}, \quad \text{for } z \neq 0.$$

However, one very important difference between the set of real numbers and the set of complex numbers is that, unlike the real numbers, the complex numbers are not *ordered*.

Recall that, for any two real numbers a and b, exactly one of the three properties

$$a < b, \quad a = b, \quad \text{or} \quad a > b$$

is true; this is what we mean by saying that the real numbers are ordered. But this is not the case for the complex numbers. For example, given the complex numbers $1 + 2i$ and $-1 + 3i$, we cannot say that one of the following properties is true:

$$1 + 2i > -1 + 3i \quad \text{or} \quad 1 + 2i = -1 + 3i \quad \text{or} \quad 1 + 2i < -1 + 3i.$$

Indeed, inequalities involving complex numbers make sense only if they are inequalities between *real* quantities, such as the moduli of the complex numbers. (Note that 'moduli' is the plural of 'modulus'.) For example, inequalities such as

$$|z - 2i| \leq 3 \quad \text{or} \quad \operatorname{Re} z > 5$$

are valid.

2.3 Polar form

You have seen that the complex number $x + iy$ corresponds to the point (x, y) in the complex plane. This correspondence enables us to give an alternative description of complex numbers, using so-called *polar form*. This form is particularly useful when we discuss properties related to multiplication and division of complex numbers.

Polar form is obtained by noting that the point in the complex plane associated with the non-zero complex number $z = x + iy$ is uniquely determined by the modulus $r = |z| = \sqrt{x^2 + y^2}$, together with the angle θ (measured in an anticlockwise direction in radians) between the positive direction of the real axis and the line from the origin to the point, as shown in Figure 8. We have

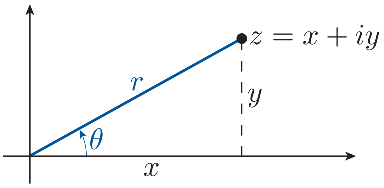


Figure 8 A complex number determined by its modulus and angle

$$x = r\cos\theta \quad \text{and} \quad y = r\sin\theta,$$

so the complex number z can be expressed as

$$z = x + iy = r(\cos\theta + i\sin\theta).$$

This description of z in terms of r and θ is not unique because the angles $\theta \pm 2\pi$, $\theta \pm 4\pi$, $\theta \pm 6\pi$, ..., also determine the same complex number. However, if we restrict the angle θ to lie in the interval $(-\pi, \pi]$, then the description *is* unique. (Some texts restrict θ to lie in the interval $[0, 2\pi)$.)

Note that for the complex number 0, which is represented in the complex plane by the origin, the value of r is 0, and θ is not defined.

Definitions

A non-zero complex number $z = x + iy$ is in **polar form** if it is expressed as

$$z = r(\cos\theta + i\sin\theta),$$

where $r = |z|$ and θ is any angle (measured in radians anticlockwise) between the positive direction of the x-axis and the line joining z to the origin.

Such an angle θ is called an **argument** of the complex number z, and is denoted by $\arg z$. The **principal argument** of z is the value of $\arg z$ that lies in the interval $(-\pi, \pi]$, and is denoted by $\operatorname{Arg} z$.

The term *principal argument* is a shortened form of the more conventional 'principal *value of the* argument'. Some texts use $r \operatorname{cis}\theta$, $r\angle\theta$ or $\langle r, \theta\rangle$ as shorthand for $r(\cos\theta + i\sin\theta)$.

Sometimes we refer to $z = x + iy$ as the **Cartesian form** of z, to distinguish it from the polar form.

We now look at how to convert a complex number from polar form to Cartesian form, and vice versa.

When carrying out such conversions, it is useful to remember the values in the table below, as these will help you in some special cases. You may find it easier to remember the triangles in Figure 9, from which you can work out most of the values in the table.

Sines and cosines of special angles

θ	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
$\sin\theta$	0	$\frac{1}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{\sqrt{3}}{2}$	1
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$	0

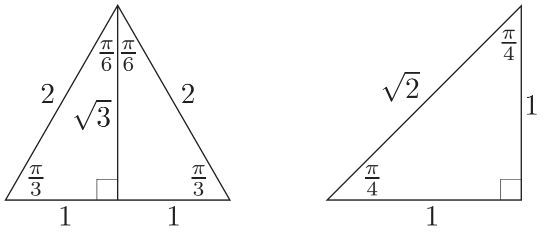


Figure 9 Triangles for finding sines and cosines of special angles

The following trigonometric identities are also helpful; they are included in the module Handbook.

Useful trigonometric identities

For any $\theta \in \mathbb{R}$,

$$\sin(\pi - \theta) = \sin\theta, \qquad \sin(-\theta) = -\sin\theta,$$
$$\cos(\pi - \theta) = -\cos\theta, \qquad \cos(-\theta) = \cos\theta.$$

You may be able to remember these identities by roughly sketching graphs of the sine and cosine functions, and using their symmetry. For example, we can sketch the sine function as in Figure 10.

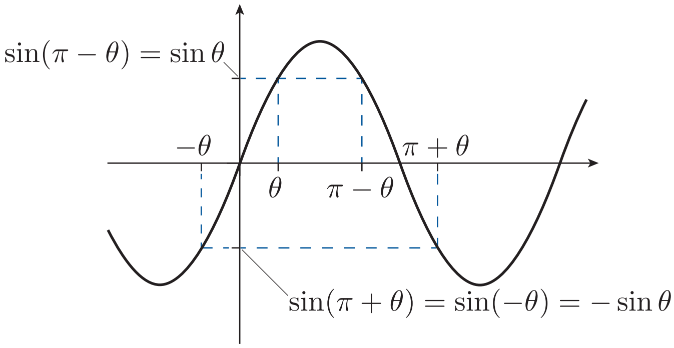


Figure 10 A sketch of the sine function for working out symmetry identities

Converting a complex number from polar form to Cartesian form is straightforward: we simply use the equations

$$x = r\cos\theta, \quad y = r\sin\theta$$

as above to find x and y given r and θ. This is demonstrated in the following worked exercise.

Worked Exercise A29

Express each of the following complex numbers in Cartesian form.

(a) $3\left(\cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3}\right)$ (b) $\cos\left(-\dfrac{\pi}{6}\right) + i\sin\left(-\dfrac{\pi}{6}\right)$

Solution

(a) Here $r = 3$ and $\theta = \pi/3$. Thus the required form is $x + iy$, where

$$x = 3\cos\frac{\pi}{3} = 3 \times \tfrac{1}{2} = \tfrac{3}{2}$$

and

$$y = 3\sin\frac{\pi}{3} = 3 \times \frac{\sqrt{3}}{2} = \frac{3\sqrt{3}}{2}.$$

The Cartesian form is therefore $\tfrac{3}{2}(1 + i\sqrt{3})$.

(b) Here $r = 1$ and $\theta = -\pi/6$. Thus the required form is $x + iy$, where

$$x = \cos\left(-\frac{\pi}{6}\right) = \cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$$

and

$$y = \sin\left(-\frac{\pi}{6}\right) = -\sin\frac{\pi}{6} = -\tfrac{1}{2}.$$

The Cartesian form is therefore $\tfrac{1}{2}(\sqrt{3} - i)$.

Exercise A72

Express each of the following complex numbers in Cartesian form.

(a) $2\left(\cos\dfrac{\pi}{2}+i\sin\dfrac{\pi}{2}\right)$ (b) $4\left(\cos\left(-\dfrac{2\pi}{3}\right)+i\sin\left(-\dfrac{2\pi}{3}\right)\right)$

To convert a non-zero complex number z from Cartesian form $x+iy$ to polar form $r(\cos\theta+i\sin\theta)$, we first find the modulus r using the formula

$$r=\sqrt{x^2+y^2}.$$

Then we find the principal argument θ; recall that this is the angle in the interval $(-\pi,\pi]$ measured in an anticlockwise direction (in radians) between the positive direction of the real axis and the line from the origin to z.

If z is either real or imaginary, then it lies on one of the axes and has principal argument 0, $\pi/2$, π or $-\pi/2$, as shown in Figure 11.

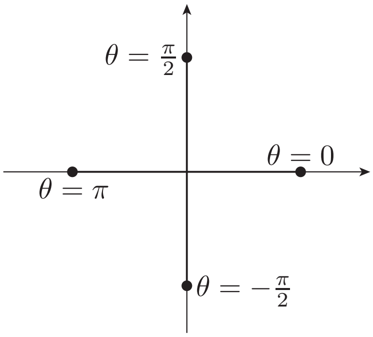


Figure 11 The principal argument θ when z is real or imaginary

Otherwise, to find the principal argument θ we need to solve the equations

$$\cos\theta=\frac{x}{r}\quad\text{and}\quad\sin\theta=\frac{y}{r},\quad\text{where }\theta\in(-\pi,\pi].$$

We can do this by first finding the acute angle ϕ that satisfies the related equation

$$\cos\phi=\frac{|x|}{r}\quad\left(\text{or, equivalently, }\sin\phi=\frac{|y|}{r}\text{ or }\tan\phi=\left|\frac{y}{x}\right|\right).$$

This acute angle ϕ is the angle at the origin in the right-angled triangle formed by drawing the perpendicular from z to the real axis, as illustrated in Figure 12 in the case where z lies in the second quadrant. (Remember that the quadrants are numbered as shown in Figure 13.)

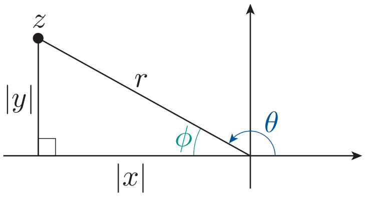


Figure 12 The angles ϕ and θ

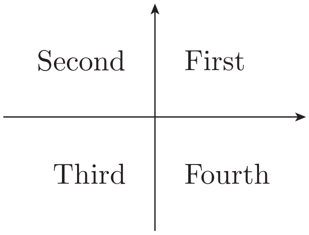


Figure 13 The quadrants of the plane

Once we have found this acute angle ϕ, we can find the principal argument θ by sketching z in the complex plane (the important thing is to get it in the correct quadrant), marking the acute angle ϕ on the sketch, and deducing the principal argument θ. For example, if z is in the third quadrant and $\phi = \pi/3$, then we can see from the sketch in Figure 14 that

$$\theta = -\left(\pi - \frac{\pi}{3}\right) = -\frac{2\pi}{3}.$$

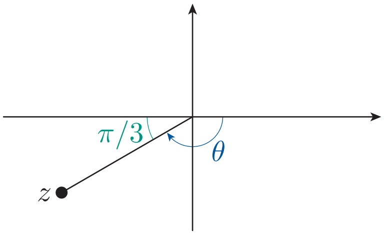


Figure 14 A complex number z in the third quadrant, with $\phi = \pi/3$

In fact, the relationship between the principal argument θ and the acute angle ϕ, for each of the four quadrants in which z can lie, is as shown in Figure 15. So, if you prefer, you can use the appropriate formula from Figure 15 to deduce θ from ϕ. You can also find the quadrant in which z lies by using the values of x and y, without having to sketch z in the complex plane.

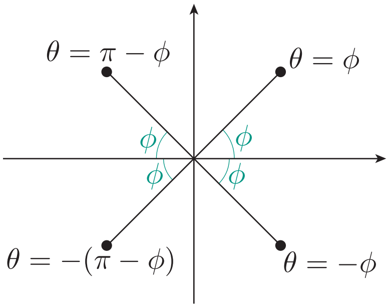


Figure 15 The relationship between θ and ϕ for each quadrant

Both methods for finding θ are illustrated in the next worked exercise.

Worked Exercise A30

Express each of the following complex numbers in polar form, using the principal argument.

(a) $2 + 2i$ (b) $-\frac{1}{2}(1 + i\sqrt{3})$

Solution

(a) Let $z = x + iy = 2 + 2i$, so $x = 2$ and $y = 2$.

Both x and y are positive, so z lies in the first quadrant.

Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{x^2 + y^2} = \sqrt{2^2 + 2^2} = \sqrt{8} = 2\sqrt{2}.$$

To find θ, we calculate

$$\cos\phi = \frac{|x|}{r} = \frac{2}{2\sqrt{2}} = \frac{1}{\sqrt{2}}.$$

So $\phi = \pi/4$, and z lies in the first quadrant so $\theta = \phi = \pi/4$.

The polar form of $2+2i$ in terms of the principal argument is therefore

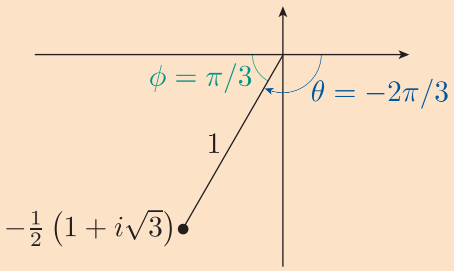
$$2\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right).$$

(b) Let $z=x+iy=-\frac{1}{2}(1+i\sqrt{3})$, so $x=-\frac{1}{2}$ and $y=-\sqrt{3}/2$.

Then $z=r(\cos\theta+i\sin\theta)$, where

$$r=\sqrt{x^2+y^2}=\sqrt{\left(-\frac{1}{2}\right)^2+\left(-\frac{\sqrt{3}}{2}\right)^2}=1.$$

A sketch helps here. We have added on the values for ϕ and θ although they are not known when this is first sketched.



To find θ, we calculate

$$\cos\phi=\frac{|x|}{r}=\frac{|-\frac{1}{2}|}{1}=\tfrac{1}{2}.$$

So $\phi=\pi/3$, and from the drawing we see that $\theta=-(\pi-\phi)=-2\pi/3$.

The polar form of $-\frac{1}{2}(1+i\sqrt{3})$ in terms of the principal argument is therefore

$$\cos\left(-\frac{2\pi}{3}\right)+i\sin\left(-\frac{2\pi}{3}\right).$$

Exercise A73

For each of the following complex numbers, draw a diagram showing its location in the complex plane. Express the complex number in polar form using the principal argument, and mark this argument and the modulus on your diagram.

(a) $-1+i$ (b) $1-i\sqrt{3}$ (c) -5

The following pair of trigonometric identities simplify multiplication of complex numbers in polar form; they are included in the module Handbook.

More useful trigonometric identities

For any $\theta_1, \theta_2 \in \mathbb{R}$,

$$\sin(\theta_1 + \theta_2) = \sin\theta_1 \cos\theta_2 + \cos\theta_1 \sin\theta_2,$$
$$\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2.$$

Let

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \quad \text{and} \quad z_2 = r_2(\cos\theta_2 + i\sin\theta_2).$$

Then, by the trigonometric identities above,

$$\begin{aligned} z_1 z_2 &= r_1(\cos\theta_1 + i\sin\theta_1) \times r_2(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) \\ &= r_1 r_2(\cos\theta_1\cos\theta_2 + i\sin\theta_1\cos\theta_2 + i\cos\theta_1\sin\theta_2 + i^2\sin\theta_1\sin\theta_2) \\ &= r_1 r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)) \\ &= r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \end{aligned}$$

That is, to multiply two complex numbers in polar form, we *multiply* their moduli and *add* their arguments:

$$z_1 z_2 = r_1 r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)). \tag{1}$$

Worked Exercise A31

Find the product $z_1 z_2$ in polar form using the principal argument for the following complex numbers z_1 and z_2:

$$z_1 = 2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \quad \text{and} \quad z_2 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right).$$

Solution

$$\begin{aligned} 2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) &\times 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) \\ &= 2\times 3\left(\cos\left(\frac{\pi}{4}+\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{4}+\frac{\pi}{3}\right)\right) \\ &= 6\left(\cos\frac{7\pi}{12} + i\sin\frac{7\pi}{12}\right). \end{aligned}$$

The principal argument lies in the interval $(-\pi, \pi]$.

Since $-\pi < 7\pi/12 \le \pi$, the above expression gives the product $z_1 z_2$ in polar form using the principal argument.

We can also use formula (1) for the product of two complex numbers in polar form to establish a similar formula for the *quotient* of two complex numbers. Specifically, we show that if

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1) \quad \text{and} \quad z_2 = r_2(\cos\theta_2 + i\sin\theta_2),$$

with $z_2 \neq 0$, which implies that $r_2 \neq 0$, then z_1/z_2 is the complex number

$$z = r(\cos\theta + i\sin\theta), \text{ where } r = r_1/r_2 \text{ and } \theta = \theta_1 - \theta_2.$$

To see this, notice that since $r_1 = rr_2$ and $\theta_1 = \theta + \theta_2$ it follows from the discussion above that $z_1 = zz_2$. Hence $z_1/z_2 = z$, as required.

That is, to divide a complex number z_1 by another complex number z_2, we divide the modulus of z_1 by the modulus of z_2, and subtract the argument of z_2 from the argument of z_1:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\theta_1 - \theta_2) + i\sin(\theta_1 - \theta_2)), \text{ where } z_2 \neq 0. \tag{2}$$

Worked Exercise A32

Find the quotient z_1/z_2 in polar form using the principal argument for the following complex numbers z_1 and z_2:

$$z_1 = 2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \quad \text{and} \quad z_2 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right).$$

Solution

$$\begin{aligned}\frac{2\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)}{3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)} &= \frac{2}{3}\left(\cos\left(\frac{\pi}{4} - \frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{4} - \frac{\pi}{3}\right)\right)\\ &= \frac{2}{3}\left(\cos\left(-\frac{\pi}{12}\right) + i\sin\left(-\frac{\pi}{12}\right)\right).\end{aligned}$$

The principal argument lies in the interval $(-\pi, \pi]$.

Since $-\pi < -\pi/12 \leq \pi$, the above expression gives the quotient z_1/z_2 in polar form using the principal argument.

In particular, if $z = r(\cos\theta + i\sin\theta)$ with $r \neq 0$, then the reciprocal of z is

$$\begin{aligned}\frac{1}{z} &= \frac{1}{r}(\cos(0 - \theta) + i\sin(0 - \theta))\\ &= \frac{1}{r}(\cos(-\theta) + i\sin(-\theta))\\ &= \frac{1}{r}(\cos\theta - i\sin\theta),\end{aligned}$$

so we have the identity

$$\frac{1}{z} = \frac{1}{r}(\cos(-\theta) + i\sin(-\theta)). \tag{3}$$

The methods that you have seen for multiplying complex numbers in polar form can be generalised to apply to a product of several complex numbers. These methods are as summarised in the box below.

Product and quotient in polar form

- To multiply two (or more) complex numbers given in polar form, multiply their moduli and add their arguments.
- To divide a complex number z_1 by a non-zero complex number z_2 when both are given in polar form, divide the modulus of z_1 by the modulus of z_2, and subtract the argument of z_2 from the argument of z_1.

If you want the *principal* argument of a product or quotient, then you may need to add or subtract integer multiples of 2π from the argument calculated, to obtain an angle in the interval $(-\pi, \pi]$.

Exercise A74

Determine the product z_1z_2 and the quotient z_1/z_2 in polar form using the principal argument for the following complex numbers.

(a) $z_1 = 4\left(\cos\left(-\frac{\pi}{6}\right) + i\sin\left(-\frac{\pi}{6}\right)\right)$ and $z_2 = \frac{1}{2}\left(\cos\frac{7\pi}{8} + i\sin\frac{7\pi}{8}\right)$.

(b) $z_1 = 3\left(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}\right)$ and $z_2 = \frac{1}{2}\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)$.

Exercise A75

Let $z_1 = -1 + i$, $z_2 = 1 - i\sqrt{3}$ and $z_3 = -5$.

Express $z_1z_2z_3$ and $\dfrac{z_2z_3}{z_1}$ in polar form using the principal argument.

(You found in Exercise A73 that $-1 + i = \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right)$, $1 - i\sqrt{3} = 2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right)$, and $-5 = 5(\cos\pi + i\sin\pi)$.)

2.4 Complex roots of polynomials

We begin this section with a reminder of what we mean by the word 'root'. In this unit, we use this term in two different, but related, senses, as given below. You met the first of these in Subsection 1.4.

Definitions

If $p(z)$ is a polynomial, then the solutions of the polynomial equation $p(z) = 0$ are called the **roots** of $p(z)$.

If a is a complex number, then the solutions of the equation $z^n = a$ are called the nth **roots** of a.

The two uses of the word 'root' are related as follows: the nth roots of a are the roots of the polynomial $z^n - a$.

Recall that the roots of a polynomial are also called its **zeros**.

In this subsection we look at how to find the nth roots of any complex number, and we consider the roots of polynomial equations more generally.

We can obtain a useful result by considering what happens when we multiply together n copies of the same complex number in polar form. If $z = r(\cos\theta + i\sin\theta)$, then by the method that you saw above for multiplying complex numbers in polar form, we obtain

$$(r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta), \quad \text{for } n \geq 1. \tag{4}$$

As before, the argument $n\theta$ may not be the *principal* argument of $(\cos\theta + i\sin\theta)^n$, so we may need to add or subtract integer multiples of 2π to obtain an angle in the interval $(-\pi, \pi]$. This is illustrated in the next worked exercise.

Worked Exercise A33

Find z^4, where $z = -1 + i$.

Solution

Find the polar form of z, then apply equation (4).

From Exercise A73(a), we have

$$-1 + i = \sqrt{2}\left(\cos\left(\frac{3\pi}{4}\right) + i\sin\left(\frac{3\pi}{4}\right)\right),$$

so

$$\begin{aligned}(-1+i)^4 &= (\sqrt{2})^4\left(\cos\left(4 \times \frac{3\pi}{4}\right) + i\sin\left(4 \times \frac{3\pi}{4}\right)\right)\\ &= 4(\cos 3\pi + i\sin 3\pi)\end{aligned}$$

We need the principal argument, so subtract 2π to get a value in $(-\pi, \pi]$.

$$= 4(\cos\pi + i\sin\pi) = -4.$$

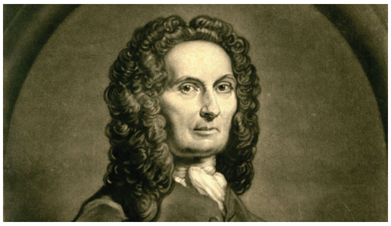
Therefore $z^4 = -4$.

You have seen that equation (4) holds for all $n \geq 1$; in fact, it is true for all integers. This follows from a result known as *de Moivre's Theorem*.

Theorem A4 de Moivre's Theorem

If $z = \cos\theta + i\sin\theta$, then for any $n \in \mathbb{Z}$,

$$z^n = (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta.$$



Abraham de Moivre

Abraham de Moivre (1667–1754) was a French mathematician who worked in England. He was part of the Huguenot flight from France after the revocation of the Edict of Nantes in 1685 and is first recorded as being in England in late 1686. De Moivre's most important work is *The Doctrine of Chances* (1718), the first textbook for the calculus of probabilities.

To see that de Moivre's Theorem is true for all integers, we need to also consider the cases where $n = 0$ and n is negative. We look at these cases separately, as follows.

For $n = 0$, we have

$$(\cos\theta + i\sin\theta)^0 = 1,$$

and

$$\begin{aligned}\cos(0\times\theta) + i\sin(0\times\theta) &= \cos 0 + i\sin 0\\ &= 1.\end{aligned}$$

Thus the result holds for $n = 0$.

For $n = -m$, where m is a positive integer, we have

$$\begin{aligned}(\cos\theta + i\sin\theta)^n &= (\cos\theta + i\sin\theta)^{-m}\\ &= \frac{1}{(\cos\theta + i\sin\theta)^m},\end{aligned}$$

and we know that $(\cos\theta + i\sin\theta)^m = \cos(m\theta) + i\sin(m\theta)$, since m is a positive integer. Therefore

$$\begin{aligned}(\cos\theta + i\sin\theta)^n &= \frac{1}{\cos(m\theta) + i\sin(m\theta)}\\ &= \cos(-m\theta) + i\sin(-m\theta) \quad \text{(by formula (3))}\\ &= \cos n\theta + i\sin n\theta,\end{aligned}$$

as required.

One application of de Moivre's Theorem is in finding the nth roots of complex numbers; that is, in solving equations of the form $z^n = a$, where $a \in \mathbb{C}$. Before you see how to do this, you are asked in the next exercise to use the theorem to verify some solutions of such an equation.

Exercise A76

(a) Write down the complex number 1 in polar form.

(b) Use de Moivre's Theorem to show that each of the three complex numbers with polar forms

$$\cos 0 + i\sin 0, \quad \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \quad \text{and} \quad \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$$

satisfies the equation $z^3 = 1$.

(c) Write down the three solutions to the equation $z^3 = 1$ given in part (b) in Cartesian form.

The solution to Exercise A76 verifies that the three given complex numbers are solutions of the equation $z^3 = 1$. However, what we really want is a method that will enable us to find solutions of such an equation. Fortunately, de Moivre's Theorem enables us to do this. The method is demonstrated in the next worked exercise.

Worked Exercise A34

Solve the equation $z^3 = -27$. Find the Cartesian form of each solution, and sketch the solutions in the complex plane.

Solution

Write the variable z in polar form, in terms of a variable modulus r and a variable argument θ. Also write the number on the right-hand side of the equation in polar form.

Let $z = r(\cos\theta + i\sin\theta)$. Also, $-27 = 27(\cos\pi + i\sin\pi)$. So the equation $z^3 = 27$ is

$$r^3(\cos\theta + i\sin\theta)^3 = 27(\cos\pi + i\sin\pi).$$

Use de Moivre's Theorem to find the polar form of the left-hand side.

By de Moivre's Theorem, the equation can be written as

$$r^3(\cos 3\theta + i\sin 3\theta) = 27(\cos\pi + i\sin\pi).$$

Find r by comparing moduli on each side.

Comparing moduli gives $r^3 = 27$, so $r = 3$.

Now find θ by comparing arguments on each side. One solution for θ is obtained by taking $3\theta = \pi$. However, we could also take $3\pi,\ 5\pi,\ 7\pi,\ \ldots$ as arguments of -27, so $3\theta = 3\pi$, $3\theta = 5\pi$, $3\theta = 7\pi$, $\ldots$ also give solutions. In general, for any $k \in \mathbb{Z}$, the equation $3\theta = \pi + 2k\pi$, that is, $\theta = \dfrac{\pi}{3} + \dfrac{2k\pi}{3}$, gives a solution. However, as discussed after this worked example, we need consider only $k = 0, 1, 2$, as other values of k just repeat the same three solutions.

The possible values of θ are given by

$$\theta = \frac{\pi}{3} + \frac{2k\pi}{3}$$

for $k = 0, 1, 2$. So they are

$$\theta = \frac{\pi}{3},\ \pi,\ \frac{5\pi}{3}.$$

Write out the solutions. It is convenient to label them as z_k; that is, z_0, z_1, z_2.

Thus the solutions of the equation are

$$z_0 = 3\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right),$$
$$z_1 = 3\,(\cos\pi + i\sin\pi),$$
$$z_2 = 3\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right).$$

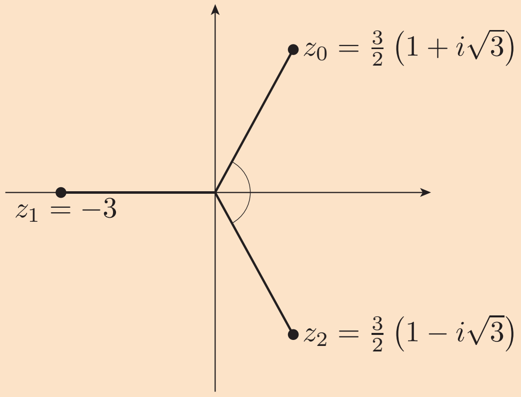
We can write z_2 using its principal argument as follows:

$$z_2 = 3\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right).$$

In Cartesian form, we have

$$z_0 = \tfrac{3}{2}(1 + i\sqrt{3}), \quad z_1 = -3, \quad z_2 = \tfrac{3}{2}(1 - i\sqrt{3}).$$

A sketch of the solutions on the complex plane is given below.


$z_0 = \frac{3}{2}\left(1 + i\sqrt{3}\right)$
$z_1 = -3$
$z_2 = \frac{3}{2}\left(1 - i\sqrt{3}\right)$

In Worked Exercise A34 we took $k = 0, 1, 2$ in the formula

$$\theta = \frac{\pi}{3} + \frac{2k\pi}{3},$$

and obtained three corresponding solutions z_0, z_1, z_2. Notice that if we take $k = 3$ in the formula, then we obtain

$$\theta = \frac{\pi}{3} + \frac{6\pi}{3} = \frac{\pi}{3} + 2\pi,$$

which gives solution z_0 again, since this value of θ differs from the argument of z_0 by an integer multiple of 2π. You can check in the same way that if we take $k = 4$ then we obtain solution z_1 again, and if we take $k = 5$ then we obtain solution z_2 again, and so on. That is, if we take $k = 0, 1, 2, 3, 4, \ldots$, in Worked Exercise A34, then after the third different solution the solutions repeat in an indefinite cycle. The same solutions are repeated if we take k to be a negative integer.

We can use the method of Worked Exercise A34 to find the solutions of any complex equation of the form

$$z^n = a,$$

where a is a known complex number. To do this, we start by writing both z and a in polar form so that, say,

$$z = r(\cos\theta + i\sin\theta) \quad \text{and} \quad a = \rho(\cos\phi + i\sin\phi),$$

where r and θ are variables whose values we must find, and ρ and ϕ are known real numbers.

Then, by de Moivre's Theorem, the equation $z^n = a$ can be written as

$$r^n(\cos n\theta + i\sin n\theta) = \rho(\cos\phi + i\sin\phi).$$

Hence we must have $r^n = \rho$, so $r = \rho^{1/n}$. Also $n\theta$ must represent the same angle as ϕ. We again use the fact that a complex number has many arguments, so adding any integer multiple of 2π to the argument ϕ of a gives the same complex number a. So we have

$$n\theta = \phi + 2k\pi, \quad \text{for any integer } k,$$

that is,

$$\theta = \frac{\phi}{n} + \frac{2k\pi}{n}, \quad \text{for any integer } k.$$

If $k = n$ we have $\theta = \phi/n + 2\pi$, which represents the same angle as ϕ/n. So taking $k = 0, 1, 2, \ldots, n-1$ will give the n different solutions of the equation $z^n = a$.

Exercise A77

(a) Use the method described above to find the six solutions of the equation $z^6 = 1$ in polar form using the principal argument.

(b) Sketch the position of each solution in the complex plane.

(c) Write down the Cartesian form of each solution.

In Exercise A77 you found the solutions of the equation $z^6 = 1$. These are known as the sixth roots of unity, and in the complex plane they are equally spaced around the circle of radius 1, centre the origin. More generally, the solutions of the equation $z^n = 1$ are known as the **nth roots of unity**, and in the complex plane they are equally spaced around the circle of radius 1, centre the origin. For any $n \in \mathbb{N}$, the real number 1 is always one of the nth roots of unity.

The nth roots of any complex number are also equally spaced around a circle with centre the origin, but the circle may not have radius 1 and there may not be a root on the real axis, as the following exercises illustrate.

Exercise A78

Solve the equation $z^4 = -4$, expressing your answers in Cartesian form. Mark your solutions on a diagram of the complex plane.

Exercise A79

Solve the equation $z^3 = 8i$, expressing your answers in Cartesian form. Mark your solutions on a diagram of the complex plane.

The next box summarises the method we have been using by giving a formula for the roots of a complex number.

Roots of a complex number

Let $a = \rho(\cos\phi + i\sin\phi)$ be a complex number in polar form. Then, for any $n \in \mathbb{N}$, the equation $z^n = a$ has n solutions, given by

$$z = \rho^{1/n}\left(\cos\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right) + i\sin\left(\frac{\phi}{n} + \frac{2k\pi}{n}\right)\right),$$

for $k = 0, 1, \ldots, n-1$.

This result gives the n solutions of any equation of the form $z^n = a$, where a is a non-zero complex number. Now the equation $z^n = a$, which can be written as $z^n - a = 0$, is an example of a polynomial equation whose coefficients, 1 and $-a$, are complex numbers. Other examples of polynomial equations with complex coefficients are

$$z^2 + (1+i)z + i = 0$$

and

$$(1+i)z^5 + 2iz^3 - 3z^2 + (1-2i)z - 1 = 0.$$

It can be shown that the following result holds; the proof is not included in this module.

Theorem A5 The Fundamental Theorem of Algebra

Every polynomial equation

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0,$$

where $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{C}$ and $a_n \neq 0$, has at least one solution in $\mathbb{C}$.

We say that a number system is **algebraically closed** if every polynomial equation with coefficients in this system has a solution in this system. Therefore, unlike the reals and the rationals, the complex numbers are an algebraically closed system of numbers.

In 1799 Carl Friedrich Gauss (1777–1855), one of the greatest mathematicians of all time, published what is often considered to be the first satisfactory proof of the Fundamental Theorem of Algebra. However, Gauss himself was not satisfied with the proof and over the course of the next fifty years published three further proofs. Later Gauss's original proof, which was mainly geometrical, was shown to be incomplete. In 1920 the gap in Gauss's proof was filled by the Russian mathematician Alexander Ostrowski (1893–1986).

Carl Friedrich Gauss

Alexander Ostrowski

Although we know from the Fundamental Theorem of Algebra that every polynomial equation with coefficients in $\mathbb{C}$ has at least one solution in $\mathbb{C}$, finding solutions of such polynomial equations is not easy. However, there are a few theorems that can help us do this in some special cases.

One of these theorems is the Factor Theorem (Theorem A2), which you met for polynomials where the number system is $\mathbb{R}$ in Subsection 1.4, but is also true if the number system is $\mathbb{C}$, as stated below.

Theorem A6 Factor Theorem (in $\mathbb{C}$)

Let $p(z)$ be a polynomial with coefficients in $\mathbb{C}$, and let $\alpha \in \mathbb{C}$. Then $p(\alpha) = 0$ if and only if $z - \alpha$ is a factor of $p(z)$.

In this statement of the theorem, the letter z has been used in place of x, as this is the label usually used for a complex variable. The proof is otherwise exactly the same as the proof of the theorem in $\mathbb{R}$, which you will see in Unit A3.

The next theorem is also useful. It can be deduced from the Fundamental Theorem of Algebra and the Factor Theorem. The proof of this follows in a similar way to the proof of Theorem A3 that you will see in Unit A3.

Theorem A7

Every polynomial

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0,$$

where $n \geq 1$ and the coefficients are in $\mathbb{C}$, with $a_n \neq 0$, has a factorisation

$$p(z) = a_n(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n),$$

where the complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the roots (not necessarily distinct) of $p(z)$.

Together Theorems A5 and A7 tell us that a polynomial equation of degree n with coefficients in $\mathbb{C}$ has at least one solution in $\mathbb{C}$, but can have no more than n solutions (all in $\mathbb{C}$). Moreover, if 'repeated' solutions are counted separately, then a polynomial equation of degree n with coefficients in $\mathbb{C}$ has *exactly* n solutions (all in $\mathbb{C}$). For example, the polynomial equation

$$(z - 1)^3 (z + 4)^2 (z - i) = 0$$

has degree six and has exactly six solutions: the solution 1 is counted three times, the solution -4 is counted twice and the solution i is counted once.

A third result that can help us find solutions of polynomial equations in some special cases is Theorem A8 below. You may have noticed that it follows from the quadratic formula that, for a quadratic polynomial with *real* coefficients, the roots are either both real or they occur as a complex conjugate pair.

More generally, we have the following result.

Theorem A8

If $p(z)$ is a polynomial with *real* coefficients, then whenever α is a complex root of p, so is $\overline{\alpha}$.

This result is not proved here, but you might like to try to prove it yourself; it is included as a 'challenging' exercise in the additional exercises booklet for this unit. In addition, the factors $z - \alpha$ and $z - \overline{\alpha}$ of $p(z)$ can be combined to give a real quadratic factor of $p(z)$, namely

$$(z - \alpha)(z - \overline{\alpha}) = z^2 - (\alpha + \overline{\alpha})z + \alpha\overline{\alpha},$$

which has real coefficients, since $\alpha + \overline{\alpha} = 2 \operatorname{Re} \alpha$ and $\alpha\overline{\alpha} = |\alpha|^2$.

Worked Exercise A35

(a) Show that $z = i$ is a root of the polynomial

$$p(z) = z^4 - 3z^3 + 2z^2 - 3z + 1.$$

(b) Hence find all the roots of $p(z)$.

Solution

(a) Check that $p(i) = 0$.

We have

$$\begin{aligned} p(i) &= i^4 - 3i^3 + 2i^2 - 3i + 1 \\ &= 1 + 3i - 2 - 3i + 1 \\ &= 0, \end{aligned}$$

so i is a root of $p(z)$.

(b) The polynomial $p(z)$ has *real* coefficients, so for each complex root α, the complex conjugate $\overline{\alpha}$ is also a root.

Since p has real coefficients, $z = -i$ is also a root of $p(z)$, so $(z - i)(z + i) = z^2 + 1$ is a factor of $p(z)$.

We have $z^4 - 3z^3 + 2z^2 - 3z + 1 = (z^2 + 1)(az^2 + bz + c)$. Equating the coefficients of z^4, z^3 and the constant term in this equation gives $a = 1$, $b = -3$ and $c = 1$.

By equating coefficients, we obtain

$$z^4 - 3z^3 + 2z^2 - 3z + 1 = (z^2 + 1)(z^2 - 3z + 1).$$

So the remaining two roots of $p(z)$ are the solutions of the equation $z^2 - 3z + 1 = 0$.

Using the quadratic formula, we have

$$z = \frac{3 \pm \sqrt{9 - 4}}{2} = \frac{3 \pm \sqrt{5}}{2}.$$

Hence the four roots of $p(z)$ are i, $-i$, $\frac{1}{2}(3 + \sqrt{5})$ and $\frac{1}{2}(3 - \sqrt{5})$.

Exercise A80

(a) Show that $z = 2i$ is a root of the polynomial

$$p(z) = z^4 - 2z^3 + 7z^2 - 8z + 12.$$

(b) Hence find all the roots of $p(z)$.

Exercise A81

Find, in the form $a_n z^n + \cdots + a_1 z + a_0$, a polynomial whose roots are 1, -2, $3i$ and $-3i$.

2.5 The complex exponential function

The real exponential function $f(x) = e^x$, also written as $f(x) = \exp x$, has the following properties:

$$e^0 = 1, \quad e^x e^y = e^{x+y}, \quad 1/e^x = e^{-x}, \quad \text{for all } x, y \in \mathbb{R}.$$

We will consider the real function $f(x) = e^x$ in more detail in the analysis units (Books D and F), but here we extend the definition of this function to define a function $f(z) = e^z$ whose domain and codomain are $\mathbb{C}$.

We expect complex powers of e to satisfy the same basic properties as real powers of e. So, for example, we expect that

$$e^{z_1} e^{z_2} = e^{z_1+z_2} \quad \text{and} \quad 1/e^z = e^{-z}, \quad \text{for all } z, z_1, z_2 \in \mathbb{C}.$$

It turns out that, if this is to be achieved, then the definition of e^z has to be as follows.

Definition

If $z = x + iy$, then $e^z = e^x(\cos y + i \sin y)$.

Worked Exercise A36

Use the definition above to show that

$$e^{z_1} e^{z_2} = e^{z_1+z_2}$$

for all complex numbers z_1 and z_2.

Solution

We multiply moduli and add angles in polar form.

Suppose that $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$.

Since x_1, x_2, y_1 and y_2 are *real* numbers, the usual exponential rules apply to them.

Then, using the trigonometric identities from Subsection 2.3, we have

$$\begin{aligned} e^{z_1} e^{z_2} &= e^{x_1}(\cos y_1 + i \sin y_1) e^{x_2}(\cos y_2 + i \sin y_2) \\ &= e^{x_1} e^{x_2}(\cos y_1 + i \sin y_1)(\cos y_2 + i \sin y_2) \\ &= e^{x_1+x_2}(\cos y_1 \cos y_2 + i^2 \sin y_1 \sin y_2 \\ &\qquad\qquad + i \cos y_1 \sin y_2 + i \sin y_1 \cos y_2) \\ &= e^{x_1+x_2}(\cos y_1 \cos y_2 - \sin y_1 \sin y_2 \\ &\qquad\qquad + i(\cos y_1 \sin y_2 + \sin y_1 \cos y_2)) \\ &= e^{x_1+x_2}(\cos(y_1 + y_2) + i \sin(y_1 + y_2)) \\ &= e^{(x_1+x_2)+i(y_1+y_2)} = e^{(x_1+iy_1)+(x_2+iy_2)} \\ &= e^{z_1+z_2}. \end{aligned}$$

Exercise A82

(a) Using the definition for e^z above and de Moivre's Theorem (Theorem A4), show that

$$\frac{1}{e^z} = e^{-z}, \quad \text{for all } z \in \mathbb{C}.$$

(b) Use the results from part (a) and Worked Exercise A36 to show that $e^{z_1}/e^{z_2} = e^{z_1 - z_2}$, for all $z_1, z_2 \in \mathbb{C}$.

So the rules for multiplication and division of complex powers of e are exactly the same as those for real powers. Furthermore, when the exponent z is real, that is when $z = x + 0i$, where $x \in \mathbb{R}$, the definitions of a real and a complex power of e coincide, since

$$e^z = e^{x+i0} = e^x(\cos 0 + i \sin 0) = e^x.$$

On the other hand, if $z = 0 + iy$, where $y \in \mathbb{R}$, then the definition gives the following formula.

Euler's Formula

$$e^{iy} = \cos y + i \sin y.$$

Putting $y = \pi$ in Euler's Formula, we obtain

$$e^{i\pi} = \cos \pi + i \sin \pi = -1 + i0 = -1.$$

This equation is usually written as follows.

Euler's Identity

$$e^{i\pi} + 1 = 0.$$

This is a remarkable relationship between five important numbers: 0, 1, i, π and e.

In 1748, Leonhard Euler, in his famous *Introductio in analysin infinitorum* (Introduction to the Analysis of the Infinite), published the equations:

$$e^{+v\sqrt{-1}} = \cos v + \sqrt{-1}\sin v,$$

and

$$e^{-v\sqrt{-1}} = \cos v - \sqrt{-1}\sin v.$$

However, Euler himself never published what we now know as Euler's Identity.

Euler was also responsible for introducing the symbol i for the imaginary number with the property that $i^2 = -1$, and the symbol e to represent the base of natural logarithms, although he did not use the symbol i until 1777 and it was not published until 1794.

The formula $e^{iy} = \cos y + i\sin y$ gives us an alternative form for the expression of a complex number in polar form. If

$$z = x + iy = r(\cos\theta + i\sin\theta),$$

then we can write $\cos\theta + i\sin\theta$ as $e^{i\theta}$, so

$$z = re^{i\theta}.$$

A complex number expressed in this way is said to be in *exponential form*.

Definition

A non-zero complex number $z = x + iy = r(\cos\theta + i\sin\theta)$ is in **exponential form** if it is expressed as

$$z = re^{i\theta}.$$

Rather than using the term *exponential form*, some texts regard $re^{i\theta}$ as another version of *polar form*, since it involves the modulus and angle of the complex number.

When we use exponential form for complex numbers, de Moivre's Theorem (Theorem A4) becomes the simple result

$$(e^{i\theta})^n = e^{in\theta}, \quad \text{for all } \theta \in \mathbb{R} \text{ and all } n \in \mathbb{Z}.$$

Similarly, if $z_1 = r_1e^{i\theta_1}$ and $z_2 = r_2e^{i\theta_2}$, the rules for multiplying and dividing complex numbers become the following simple results:

$$z_1z_2 = r_1e^{i\theta_1} \times r_2e^{i\theta_2} = r_1r_2e^{i(\theta_1+\theta_2)},$$

$$\frac{z_1}{z_2} = \frac{r_1e^{i\theta_1}}{r_2e^{i\theta_2}} = \frac{r_1}{r_2}e^{i(\theta_1-\theta_2)} \quad (\text{provided } z_2 \neq 0).$$

There is also a useful formula for the complex conjugate of a complex number in exponential form, as follows.

If $z = re^{i\theta}$, then $\overline{z} = re^{-i\theta}$.

This formula can be proved as follows. If $z = re^{i\theta}$, then $z = r(\cos\theta + i\sin\theta)$, so

$$\begin{aligned}\overline{z} &= r(\cos\theta - i\sin\theta)\\ &= r(\cos(-\theta) + i\sin(-\theta))\\ &= re^{-i\theta}.\end{aligned}$$

The second line here follows from the trigonometric identities $\cos(-\theta) = \cos\theta$ and $\sin(-\theta) = -\sin\theta$.

Exercise A83

Use Euler's Identity to prove that if $z = re^{i\theta}$, then $-z = re^{i(\theta+\pi)}$.

2.6 Summary: Cartesian, polar and exponential form

You have seen in the previous subsections that certain calculations with complex numbers are considerably easier in some forms than in others. For example, if we use polar form or exponential form, then we can easily find powers using de Moivre's Theorem (Theorem A4). Here is a summary of the main features of the different forms of a complex number, and how to convert between them.

Let

$$\begin{aligned}z &= x + iy = r(\cos\theta + i\sin\theta) = re^{i\theta},\\ z_1 &= x_1 + iy_1 = r_1(\cos\theta_1 + i\sin\theta_1) = r_1e^{i\theta_1},\\ z_2 &= x_2 + iy_2 = r_2(\cos\theta_2 + i\sin\theta_2) = r_2e^{i\theta_2}.\end{aligned}$$

Complex conjugate

Cartesian form $\overline{z} = x - iy$

Polar form $\overline{z} = r(\cos\theta - i\sin\theta)$

Exponential form $\overline{z} = re^{-i\theta}$

Product

Cartesian form Use the usual rules of arithmetic to find z_1z_2.

Polar form $z_1z_2 = r_1r_2\left(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right)$

Exponential form $z_1z_2 = r_1r_2e^{i(\theta_1+\theta_2)}$

Reciprocal (In each case, $z \neq 0$.)

Cartesian form $\dfrac{1}{z} = \dfrac{1}{z} \times \dfrac{\overline{z}}{\overline{z}} = \dfrac{\overline{z}}{|z|^2}$

Polar form $\dfrac{1}{z} = \dfrac{1}{r}(\cos(-\theta) + i\sin(-\theta)) = \dfrac{1}{r}(\cos\theta - i\sin\theta)$

Exponential form $\dfrac{1}{z} = \dfrac{1}{r}e^{-i\theta}$

Quotient (In each case, $z_2 \neq 0$.)

Cartesian form $\dfrac{z_1}{z_2} = \dfrac{z_1}{z_2} \times \dfrac{\overline{z_2}}{\overline{z_2}} = \dfrac{z_1\overline{z_2}}{|z_2|^2}$

Polar form $\dfrac{z_1}{z_2} = \dfrac{r_1}{r_2}(\cos(\theta_1-\theta_2) + i\sin(\theta_1-\theta_2))$

Exponential form $\dfrac{z_1}{z_2} = \dfrac{r_1}{r_2}e^{i(\theta_1-\theta_2)}$

Converting polar and exponential form to Cartesian form

Use the equations

$$x = r\cos\theta, \quad y = r\sin\theta.$$

Converting Cartesian form to polar and exponential form

Find the modulus r, using $r = |z| = \sqrt{x^2+y^2}$.

Mark z on a sketch of the complex plane. Find the acute angle ϕ at the origin in the right-angled triangle formed by drawing the perpendicular from z to the real axis, using

$$\cos\phi = \frac{|x|}{r}.$$

Hence find the principal argument.

3 Modular arithmetic

In this section you will see how we can do arithmetic with finite sets of integers. We do this by using *modular arithmetic*, which you should have met in your previous studies. This type of arithmetic is important in number theory (the study of the integers) and in cryptography. You will use it frequently in the group theory units of this module (Books B and E).

3.1 The Division Theorem

If we divide one positive integer by another we obtain a *quotient* and a *remainder*. For example, 29 divided by 4 gives quotient 7 and remainder 1 because $29 = 7 \times 4 + 1$. If we divide any positive integer by 4, the remainder will be one of the numbers 0, 1, 2, 3.

This idea can be extended to the division of a negative integer by a positive integer. For example, -19 divided by 4 gives quotient -5 and remainder 1 because $-19 = (-5) \times 4 + 1$. If we divide any negative integer by 4, the remainder is again one of the numbers 0, 1, 2, 3.

This result can be generalised to the following theorem.

Theorem A9 Division Theorem

Let a and n be integers, with $n > 0$. Then there are unique integers q and r such that

$$a = qn + r, \quad \text{with } 0 \leq r < n.$$

We say that dividing a by the **divisor** n gives the **quotient** q and **remainder** r.

A formal proof of Theorem A9 is not given here, but the theorem can be illustrated as follows. We mark integer multiples of n along the real line as shown in Figure 16, and then observe in which of the resulting intervals of length n the integer a lies. Suppose that a lies in the interval $[qn, (q+1)n)$, so that $qn \leq a < (q+1)n$, as illustrated.

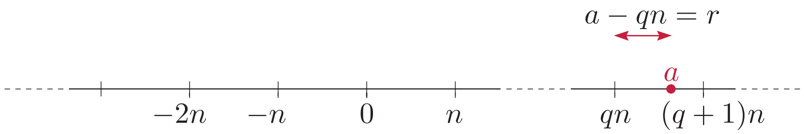


Figure 16 The number a in the interval $[qn, (q+1)n)$

Then, if we let $r = a - qn$, we have $a = qn + r$ and $0 \leq r < n$, which is the required result.

Exercise A84

For each of the following integers a and n, find the quotient and remainder on division of a by n.

(a) $a = 65, \quad n = 7$ (b) $a = -256, \quad n = 13$

Exercise A85

(a) What are the possible remainders on division of an integer by 7?

(b) Find two positive and two negative integers all of which have remainder 3 on division by 7.

3.2 Congruence

The Division Theorem (Theorem A9) tells us that, when we divide any integer by a positive integer n, the set of possible remainders is $\{0, 1, 2, \ldots, n-1\}$. Integers that differ by a multiple of n have the same remainder on division by n and are, in this sense, 'the same' as each other. We now introduce some notation and terminology for this idea of 'sameness', which is known as *congruence*.

Definitions

Let n be a positive integer. Two integers a and b are **congruent modulo n** if $a - b$ is a multiple of n; that is, if a and b have the same remainder on division by n.

In symbols we write

$$a \equiv b \pmod{n}.$$

Such a statement is called a **congruence**, and n is called the **modulus** of the congruence.

The word 'modulus' here has a different meaning from its use to mean the 'size' of a real number or a complex number. This different usage reminds us that it is always important to interpret technical terms according to their context.

We read '$a \equiv b \pmod{n}$' as 'a is congruent to b modulo n'.

The terms ‘congruent’ and ‘modulus’, together with the symbol for congruence, all appear for the first time in Gauss’s classic text *Disquisitiones Arithmeticae* (Arithmetical Investigations) of 1801, the work which, in the words of historian Olaf Neumann, ‘transformed number theory from a scattering of islands into an established continent of mathematics.’

Worked Exercise A37

Which of the following congruences are true, and which are false?

(a) $27 \equiv 5 \pmod{11}$ (b) $14 \equiv -6 \pmod{3}$

(c) $343 \equiv 207 \pmod{68}$ (d) $1 \equiv -1 \pmod{2}$

Solution

It is often simplest to check a congruence $a \equiv b \pmod{n}$ by considering the difference $a - b$.

(a) $27 - 5 = 22$, which is a multiple of 11, so this congruence is true.

Alternatively, $27 = 2 \times 11 + 5$ and $5 = 0 \times 11 + 5$, so 27 and 5 both have remainder 5 on division by 11.

(b) $14 - (-6) = 20$, which is not a multiple of 3, so this congruence is false.

Alternatively, $14 = 4 \times 3 + 2$ and $-6 = (-2) \times 3 + 0$, so 14 has remainder 2 on division by 3, but -6 has remainder 0.

(c) $343 - 207 = 136 = 2 \times 68$, so this congruence is true.

Alternatively, $343 = 5 \times 68 + 3$ and $207 = 3 \times 68 + 3$, so 343 and 207 both have remainder 3 on division by 68.

(d) $1 - (-1) = 2$, so this congruence is true.

Alternatively, both 1 and -1 have remainder 1 on division by 2.

Exercise A86

Find the remainder on division by 17 of each of the numbers 25, 53, -15, 3 and 127, and state any congruences modulo 17 that exist between these numbers.

We shall need to use some properties of congruences in the following sections, so we state these properties here. This may seem a long list, but these properties are quite simple; in fact, they are what you might expect.

Theorem A10 Properties of congruences

Let n and m be positive integers, and let a, b, c, d be integers. The following properties hold.

Reflexivity $a \equiv a \pmod{n}$.

Symmetry If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

Transitivity If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Addition If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

Multiplication If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Powers If $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$.

To see why these properties hold, we use the definition of congruence: two integers a and b are congruent modulo n if $a - b$ is a multiple of n.

The reflexive property holds because $a - a = 0 = 0 \times n$, so we have $a \equiv a \pmod{n}$.

To see why the symmetric property holds, suppose that $a \equiv b \pmod{n}$, so $a - b = kn$ for some integer k. But $b - a = -(a - b)$, so $b - a = (-k)n$. Since $-k$ is also an integer, it follows that $b \equiv a \pmod{n}$.

We can see that the transitive property holds in a similar way. Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then $a - b = kn$ and $b - c = ln$ for some integers k and l. Hence

$$a - c = a - b + b - c = kn + ln = (k + l)n.$$

Since $k + l$ is an integer, it follows that $a \equiv c \pmod{n}$.

In the next worked exercise we prove that the addition property holds, and you are asked to prove the multiplication property in Exercise A87.

Worked Exercise A38

Prove that the addition property for congruences holds:

$$\text{if } a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n}, \text{ then } a + c \equiv b + d \pmod{n}.$$

Solution

Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $a - b = kn$ and $c - d = ln$ for some integers k and l. Hence $a = b + kn$ and $c = d + ln$, so

$$a + c = b + kn + d + ln = b + d + (k + l)n.$$

Therefore $(a + c) - (b + d) = (k + l)n$. Since $k + l$ is an integer, it follows that $a + c \equiv b + d \pmod{n}$. Thus the addition property holds.

Exercise A87

Prove that the multiplication property for congruences holds:

if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

The powers property is obtained by applying the multiplication property repeatedly. Suppose that $a \equiv b \pmod{n}$. Then the multiplication property gives

$$a^2 \equiv b^2 \pmod{n}.$$

We can now apply the multiplication property to

$$a \equiv b \pmod{n} \quad \text{and} \quad a^2 \equiv b^2 \pmod{n}.$$

to obtain

$$a^3 \equiv b^3 \pmod{n}.$$

Continuing in this way, we obtain

$$a^m \equiv b^m \pmod{n} \text{ for any } m \in \mathbb{N},$$

which is the powers property.

The properties of congruences in Theorem A10 are particularly useful when we want to find the remainder of a large integer on division by another integer, as the next worked exercise illustrates.

Worked Exercise A39

(a) Find the remainders of both 2375 and 5421 on division by 22.

(b) Find the remainder of 2375 × 5421 on division by 22.

(c) Find the remainder of $(2375)^{15}$ on division by 22.

Solution

(a) Start with 2375 and subtract or add convenient multiples of 22 until you reach an integer in $\{0, 1, 2, \dots, 21\}$. Here we can subtract 2200, then 110, then 66, then add 22.

Using the transitivity property of congruences we obtain

$$2375 \equiv 175 \equiv 65 \equiv -1 \equiv 21 \pmod{22}.$$

Do the same for 5421. We can subtract 4400, then 880, then 110, then 22.

Similarly,

$$5421 \equiv 1021 \equiv 141 \equiv 31 \equiv 9 \pmod{22}.$$

So 2375 has remainder 21 on division by 22, and 5421 has remainder 9 on division by 22.

(b) Use the multiplication property. Find integers congruent modulo 22 to 2375 and 5421 that are easier to multiply.

Using the multiplication property of congruences and the answer to part (a), we obtain

$$2375 \times 5421 \equiv 21 \times 9 \equiv -1 \times 9 \equiv -9 \equiv 13 \pmod{22},$$

so 2375 × 5421 has remainder 13 on division by 22.

(c) Use the powers property. Find an integer congruent modulo 22 to 2375 whose powers are easier to find.

Using the powers property of congruences and the answer to part (a), we obtain

$$(2375)^{15} \equiv 21^{15} \equiv (-1)^{15} \equiv -1 \equiv 21 \pmod{22},$$

so $(2375)^{15}$ has remainder 21 on division by 22.

The worked exercise above shows that there is a real advantage in using congruences, since the number $(2375)^{15}$ is too large to fit into the memory of most computers.

Exercise A88

(a) Find the remainder of both 3869 and 1685 on division by 16.

(b) Find the remainder of $3869 + 1685$ on division by 16.

(c) Find the remainder of $(3869 + 1685)^4$ on division by 16, and hence find the remainder of $(3869 + 1685)^{111}$ on division by 16.

3.3 Operations in $\mathbb{Z}_n$

The Division Theorem (Theorem A9) tells us that all the possible remainders on dividing an integer by a positive integer n lie in the set

$$\{0, 1, \ldots, n-1\}.$$

We denote this set by $\mathbb{Z}_n$. For each integer $n \geq 2$ we have a set $\mathbb{Z}_n$, and it is on these sets that we perform *modular arithmetic*. The modular addition operations $+_n$ and modular multiplication operations $\times_n$ are defined as follows.

Definitions

For any integer $n \geq 2$,

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

For a and b in $\mathbb{Z}_n$, the operations $+_n$ and $\times_n$ are defined by:

$a +_n b$ is the remainder of $a + b$ on division by n;

$a \times_n b$ is the remainder of $a \times b$ on division by n.

The integer n is called the **modulus** for this arithmetic.

We read $a +_n b$ as 'a plus b, mod n', and $a \times_n b$ as 'a times b, mod n'.

For example, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and we have

$$3 + 6 = 9, \quad \text{so } 3 +_7 6 = 2,$$
$$3 \times 6 = 18, \quad \text{so } 3 \times_7 6 = 4.$$

You have certainly met some modular arithmetic before, as the operations $+_{12}$ and $+_{24}$ are used in measuring time on 12-hour and 24-hour clocks, respectively.

Arithmetic carried out on the elements of the set $\mathbb{Z}_n$ using the operations $+_n$ and $\times_n$ is called **arithmetic modulo** n.

Exercise A89

Evaluate the following.

(a) $3 +_5 2$ (b) $4 +_{17} 5$ (c) $8 +_{16} 12$

(d) $3 \times_5 2$ (e) $4 \times_{17} 5$ (f) $8 \times_{16} 12$

You can often use the properties of congruences to help you carry out arithmetic modulo n efficiently, without using a calculator, as demonstrated in the next worked exercise. There are usually many different ways to proceed.

Worked Exercise A40

Evaluate the following.

(a) $29 \times_{31} 18$ (b) $12 \times_{26} 15$

Solution

(a) Use the fact that $29 \equiv -2 \pmod{31}$, and it is easier to multiply by -2 than by 29. Remember that the final answer needs to be an integer in $\mathbb{Z}_{31}$.

We have

$$\begin{aligned} 29 \times 18 &\equiv -2 \times 18 \\ &\equiv -36 \\ &\equiv -5 \\ &\equiv 26 \pmod{31}. \end{aligned}$$

Thus $29 \times_{31} 18 = 26$.

(b) Use the fact that to multiply by 12, we can first multiply by 2 and then by 6. The final answer needs to be an integer in $\mathbb{Z}_{26}$.

We have

$$\begin{aligned} 12 \times 15 &\equiv 6 \times 2 \times 15 \\ &\equiv 6 \times 30 \\ &\equiv 6 \times 4 \\ &\equiv 24 \pmod{26}. \end{aligned}$$

Thus $12 \times_{26} 15 = 24$.

Exercise A90

Calculate the following without using a calculator.

(a) $7 \times_{27} 26$ (b) $16 \times_{29} 14$ (c) $9 \times_{33} 15$ (d) $37 \times_{45} 23$

(e) $15 \times_{34} 6$ (f) $9 \times_{40} 18$

In Subsection 1.2 you met a list of eleven properties that are satisfied by the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers and the set $\mathbb{C}$ of complex numbers. You saw that since these three sets each satisfy all eleven properties (together with a trivial twelfth property), these sets are all *fields*. You also saw that the set $\mathbb{Z}$ of integers does not satisfy all eleven of these properties, and so is not a field. In the rest of this section we will investigate whether the sets $\mathbb{Z}_n$ satisfy these properties.

We will also investigate which equations in $\mathbb{Z}_n$ have solutions; for example, do the equations

$$x +_{12} 5 = 2, \quad 5 \times_{12} x = 7, \quad 4 \times_{12} x = 6$$

have solutions? These may look much simpler than the equations we were trying to solve in $\mathbb{C}$, but they pose interesting questions. We shall see that the answers may depend on the modulus that we are using.

Before we consider these questions further, we look at addition and multiplication tables, which provide a convenient way of studying addition and multiplication in $\mathbb{Z}_n$.

We consider addition first. Here are the addition tables for $\mathbb{Z}_4$ and $\mathbb{Z}_7$.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

In order to evaluate $4 +_7 2$, say, we look in the second table at the row labelled 4 and the column labelled 2 to obtain the answer 6.

Exercise A91

(a) Use the tables above to solve the following equations.

(i) $x +_4 3 = 2$. (ii) $x +_7 5 = 2$. (iii) $x +_4 2 = 0$. (iv) $x +_7 5 = 0$.

(b) What patterns do you notice in the tables?

Exercise A92

(a) Construct the addition table for $\mathbb{Z}_6$.

(b) Solve the equations $x +_6 1 = 5$ and $x +_6 5 = 1$.

For every integer $n \geq 2$, the additive properties of $\mathbb{Z}_n$ are the same as the additive properties of $\mathbb{R}$, as follows.

Addition in $\mathbb{Z}_n$ ($n \geq 2$)

A1 Closure For all $a, b \in \mathbb{Z}_n$,

$$a +_n b \in \mathbb{Z}_n.$$

A2 Associativity For all $a, b, c \in \mathbb{Z}_n$,

$$(a +_n b) +_n c = a +_n (b +_n c).$$

A3 Additive identity For all $a \in \mathbb{Z}_n$,

$$a +_n 0 = a = 0 +_n a.$$

A4 Additive inverses For each $a \in \mathbb{Z}_n$, there is a number $b \in \mathbb{Z}_n$ such that

$$a +_n b = 0 = b +_n a.$$

A5 Commutativity For all $a, b \in \mathbb{Z}_n$,

$$a +_n b = b +_n a.$$

The closure property (A1) follows because $a +_n b$ is the remainder on dividing $a + b$ by n, which, from the Division Theorem (Theorem A9), is in $\mathbb{Z}_n$.

The other properties can be deduced from the corresponding properties for integers. For example, we can see that the associativity property (A2) holds as follows. By definition, $(a +_n b) +_n c$ and $a +_n (b +_n c)$ are the remainders of the integers $(a + b) + c$ and $a + (b + c)$, respectively, on division by n. Since ordinary addition is associative, we have $(a + b) + c = a + (b + c)$, so

$$(a +_n b) +_n c = a +_n (b +_n c).$$

Exercise A93

By using the corresponding property for integers, prove that the commutativity property (A5) holds for $\mathbb{Z}_n$.

The additive inverses property (A4) states that *every* element of $\mathbb{Z}_n$ has an additive inverse in $\mathbb{Z}_n$. For example, 4 and 5 belong to $\mathbb{Z}_9$ and $4 +_9 5 = 0$, so 5 is an additive inverse of 4 in $\mathbb{Z}_9$ (and vice versa).

Additive inverses are sometimes written in the form $-_n a$; that is, if $a +_n b = 0$, then we write $b = -_n a$. For example, $5 = -_9 4$.

Exercise A94

(a) Use the addition table for $\mathbb{Z}_7$ (given earlier and repeated as Table 1) to complete the following table of additive inverses in $\mathbb{Z}_7$.

a	0	1	2	3	4	5	6
$-_7 a$							

(b) Complete the following table of additive inverses in $\mathbb{Z}_n$, justifying your answers.

a	0	1	2	…	r	…	$n-1$
$-_n a$							

Table 1

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Notice that each element a of $\mathbb{Z}_n$ has *exactly one* additive inverse in $\mathbb{Z}_n$, namely the integer obtained by subtracting a from n. For example, the additive inverse of 4 in $\mathbb{Z}_9$ is $9 - 4 = 5$.

The existence of additive inverses means that, as well as doing addition modulo n, we can also do **subtraction modulo** n. We define $a -_n b$ or, equivalently, $a - b \pmod{n}$, to be the remainder of $a - b$ on division by n.

For example, to find $2 -_{12} 5$, we have

$$2 - 5 = -3 \equiv 9 \pmod{12}.$$

Since $9 \in \mathbb{Z}_{12}$, it follows that

$$2 -_{12} 5 = 9.$$

3.4 Multiplicative inverses in $\mathbb{Z}_n$

In the last subsection it was stated that, for any integer $n \geq 2$, the set $\mathbb{Z}_n$ satisfies the same rules for addition modulo n as the real numbers satisfy for ordinary addition. When it comes to multiplication in $\mathbb{Z}_n$, *most* of the familiar rules for multiplication of the real numbers are true. In particular, the following properties hold.

Multiplication in $\mathbb{Z}_n$ ($n \geq 2$)

M1 Closure For all $a, b \in \mathbb{Z}_n$,

$$a \times_n b \in \mathbb{Z}_n.$$

M2 Associativity For all $a, b, c \in \mathbb{Z}_n$,

$$(a \times_n b) \times_n c = a \times_n (b \times_n c)$$

M3 Multiplicative identity For all $a \in \mathbb{Z}_n$,

$$a \times_n 1 = a = 1 \times_n a.$$

M5 Commutativity For all $a, b \in \mathbb{Z}_n$,

$$a \times_n b = b \times_n a.$$

The following property also holds.

Combining addition and multiplication in $\mathbb{Z}_n$ $(n \geq 2)$

D1 Distributivity For all $a, b, c \in \mathbb{Z}_n$,

$$a \times_n (b +_n c) = (a \times_n b) +_n (a \times_n c).$$

These properties can be shown to hold in a similar way to the additive properties. You will notice that one property is missing from the list of multiplicative properties, namely the multiplicative inverses property (M4).

We say that b is a **multiplicative inverse** of a in $\mathbb{Z}_n$ if $a, b \in \mathbb{Z}_n$ and $a \times_n b = b \times_n a = 1$. We now investigate the existence of multiplicative inverses.

Here are the multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_7$.

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\times_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The table for $\mathbb{Z}_7$ shows that, for example, $3 \times_7 5 = 5 \times_7 3 = 1$, so 5 is a multiplicative inverse of 3 in $\mathbb{Z}_7$.

Exercise A95

(a) Use the tables above to answer the following.

(i) Which elements of $\mathbb{Z}_4$ have multiplicative inverses?

(ii) Find a multiplicative inverse of every element of $\mathbb{Z}_7$ except 0.

(b) Construct a multiplication table for $\mathbb{Z}_{10}$, and determine which elements of $\mathbb{Z}_{10}$ have multiplicative inverses.

In Exercise A95, you saw that, in contrast to $\mathbb{R}$ and $\mathbb{C}$, there are some values of n for which the number system $\mathbb{Z}_n$ contains non-zero elements that do not have a multiplicative inverse.

Before we investigate further the question of which elements of each number system $\mathbb{Z}_n$ have a multiplicative inverse, note that if an element of $\mathbb{Z}_n$ *does* have a multiplicative inverse, then it has *only one*. The multiplication tables for $\mathbb{Z}_4$, $\mathbb{Z}_7$ and $\mathbb{Z}_{10}$ show that this is true for these three number systems, but it is in fact true for any $\mathbb{Z}_n$, though this is less obvious than it is for additive inverses.

To see that it is true in general, suppose that a is an element of $\mathbb{Z}_n$, for some integer $n \geq 2$, and that both b and c are multiplicative inverses of a in $\mathbb{Z}_n$. Then

$$\begin{aligned} b &= 1 \times_n b \\ &= c \times_n a \times_n b \quad (\text{since } c \times_n a = 1) \\ &= c \times_n 1 \quad (\text{since } a \times_n b = 1) \\ &= c. \end{aligned}$$

That is, b and c are in fact the *same element* of $\mathbb{Z}_n$. Thus a has just one multiplicative inverse in $\mathbb{Z}_n$. We say that the inverse of a is *unique*.

When it exists, we denote the multiplicative inverse b of an element a of $\mathbb{Z}_n$ by a^{-1} and refer to it as *the* multiplicative inverse of a in $\mathbb{Z}_n$.

Notice also that if an element a of a number system $\mathbb{Z}_n$ has a multiplicative inverse b in $\mathbb{Z}_n$, then b also has a multiplicative inverse in $\mathbb{Z}_n$, namely a. This follows from the definition of a multiplicative inverse. For example, in $\mathbb{Z}_7$, the elements 3 and 5 are inverses of each other.

Let us now turn to the question of which elements of each number system $\mathbb{Z}_n$ have a multiplicative inverse. This question is connected with the *common factors* of a and n.

Definitions

Two integers a and b have a **common factor** c, where c is a natural number, if a and b are both divisible by c.

Two integers a and b are **coprime** (or **relatively prime**) if their only common factor is 1.

The **highest common factor** (**HCF**) of two integers a and b is their largest common factor.

If two integers a and b are coprime, we also say that a is coprime to b, or that b is coprime to a.

In some texts the highest common factor of a and b is called the ‘greatest common divisor’ (GCD).

It turns out that an element a of $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$ exactly when a and n are coprime. That is, if a and n are coprime, then a has a multiplicative inverse in $\mathbb{Z}_n$, but if a and n are not coprime, then a has no multiplicative inverse.

We prove this important result later in this subsection, but first we consider how to find multiplicative inverses where they exist. Of course, we could do this by trial and error, or by writing out the multiplication table for $\mathbb{Z}_n$, but for large values of n these methods are very cumbersome. Fortunately a more efficient method exists, based on *Euclid's Algorithm*.

Euclid's Algorithm is a method for finding the highest common factor of two positive integers, first described (albeit in a different form) in Euclid's *Elements*, which dates from around 300 BCE. Given an element a of $\mathbb{Z}_n$, we can apply Euclid's Algorithm to determine whether or not a and n are coprime; if they are coprime, then we know that a has a multiplicative inverse in $\mathbb{Z}_n$, but otherwise it does not. Moreover, if a and n *are* coprime, then we can use the equations that arise from applying Euclid's Algorithm to work out the multiplicative inverse of a, using a method known as **backwards substitution**.

Euclid's Algorithm proceeds by repeatedly applying the Division Theorem, as in the following example. Suppose we want to find the highest common factor of the integers 32 and 9. We start by dividing 32 by 9, which gives quotient 3 and remainder 5, as in the equation

$$32 = 3 \times 9 + 5.$$

Next, we divide 9 by 5, giving quotient 1, remainder 4 and the equation

$$9 = 1 \times 5 + 4.$$

We continue in this way, at each step forming a new equation by dividing the *divisor* from the previous equation by the *remainder* from that equation. The complete list of equations arising from Euclid's Algorithm in this example is given below.

$$\begin{tikzcd}
32 & = & 3 & \times & 9 \arrow[dllll] & + & 5 \arrow[dll] \\
9 & = & 1 & \times & 5 \arrow[dllll] & + & 4 \arrow[dll] \\
5 & = & 1 & \times & 4 \arrow[dllll] & + & 1 \arrow[dll] \\
4 & = & 4 & \times & 1 & + & 0
\end{tikzcd}$$

We stop when the remainder is 0; giving us the last equation. We always eventually reach this stage, because the remainders decrease by at least 1 at each step. The remainder in the *second-to-last equation* is the highest common factor of the two integers we started with.

So, for example, the list of equations above shows that the highest common factor of 32 and 9 is 1; they are coprime. We conclude that the number 9 does have a multiplicative inverse in $\mathbb{Z}_{32}$.

Before we describe the process of backwards substitution and use it to find this inverse, let us see why Euclid's Algorithm works. Suppose we have two positive integers, say a_1 and a_2, and we apply the Division Theorem to obtain the equation

$$a_1 = qa_2 + a_3,$$

where $0 \leq a_3 < a_2$. This equation can be rearranged as

$$a_3 = a_1 - qa_2.$$

It follows from this rearranged equation that any integer that is a factor of both a_1 and a_2 (and so is a factor of $a_1 - qa_2$) must also be a factor of a_3. Thus any common factor of a_1 and a_2 is also a common factor of a_2 and a_3. Moreover, the unrearranged form of the equation tells us, by a similar argument, that any common factor of a_2 and a_3 must also be a common factor of a_1 and a_2. It follows that the highest common factor (HCF) of a_1 and a_2 is equal to the HCF of a_2 and a_3.

So, at each stage of Euclid's Algorithm, a pair of integers a_1, a_2 leads to another pair of integers a_2, a_3 with the same highest common factor. In the example above, we obtain the sequence of pairs

32 and 9,   9 and 5,   5 and 4,   4 and 1,   1 and 0,

and each pair has the same HCF.

The final pair of integers always has second integer 0, so its HCF is its first integer; this is the integer, say d, that appears as the remainder in the second-to-last equation. Since each pair has the same HCF, it follows that the HCF of the original pair is also d.

Euclid's Algorithm is much quicker to apply than to describe! Try it for yourself in the next exercise.

Exercise A96

Use Euclid's Algorithm to find the HCF of 201 and 81. Deduce whether or not the integer 81 has a multiplicative inverse in $\mathbb{Z}_{201}$.

If we have applied Euclid's Algorithm to find the HCF of two positive integers n and a with $n > a$, and found that the HCF is 1, we can then use the list of equations obtained from the algorithm to find the multiplicative inverse of a in $\mathbb{Z}_n$ using the method of **backwards substitution**.

To illustrate the method, let us apply it to our example of Euclid's Algorithm above: this will yield the multiplicative inverse of 9 in $\mathbb{Z}_{32}$.

The first step is to rearrange each of the equations from Euclid's Algorithm to make the remainders the subjects of the equations. (We do not need the last equation, the one with remainder 0.) This gives

$$\begin{aligned}5 &= 32 - 3 \times 9\\4 &= 9 - 1 \times 5\\1 &= 5 - 1 \times 4.\end{aligned}$$

Notice that the last equation above expresses 1 as the sum of a multiple of 5 and a multiple of 4. (One of the multiples is negative – here the multiple of 4. This will always be the case because our starting integers, here 32 and 9, are both positive.)

The goal of the backwards substitution process is to obtain an equation that expresses 1 as the sum of multiples of our original two positive integers, 32 and 9. (Again, one of these multiples must be negative.)

The backwards substitution process starts with the last equation from Euclid's Algorithm:

$$1 = 5 - 1 \times 4.$$

Next, we use the second-to-last equation from Euclid's Algorithm to substitute for the 4 in the right-hand side of this equation. We then simplify the resulting equation to express 1 as the sum of multiples of 9 and 5, like this

$$\begin{aligned}1 &= 5 - (9 - 1 \times 5)\\&= (-1 \times 9) + (2 \times 5).\end{aligned}$$

Notice that, in simplifying the equation, we treat the 9 and 5 as if they were *variables*, in the same way that we would simplify the expression $x - (y - 1x)$ to give $-1y + 2x$.

Now we repeat the process, using the third-to-last equation to substitute for the 5 in the right-hand side of *this* equation, then simplifying again to express 1 as the sum of multiples of 32 and 9:

$$\begin{aligned}1 &= (-1 \times 9) + 2 \times (32 - 3 \times 9)\\&= (2 \times 32) + (-7 \times 9).\end{aligned}$$

We continue in this way, working upwards through all the equations from Euclid's Algorithm. In this case, though, there are no more equations and we have reached our goal: an equation that expresses 1 as the sum of multiples of 32 and 9.

We are now only a few short steps from finding the multiplicative inverse of 9 in $\mathbb{Z}_{32}$.

First, we rearrange our final equation to obtain a multiple of the smaller of the two integers, 9, on the left-hand side, and a multiple of the larger integer, 32, together with the term +1, on the right-hand side:

$$(-7) \times 9 = (-2) \times 32 + 1.$$

Next, we note that it follows from this equation that

$$(-7) \times 9 \equiv 1 \pmod{32}.$$

Now $-7 \notin \mathbb{Z}_{32}$, but since $-7 \equiv 25 \pmod{32}$ and $25 \in \mathbb{Z}_{32}$, we have

$$25 \times 9 \equiv 1 \pmod{32},$$

that is

$$25 \times_{32} 9 = 1.$$

Thus we have shown that the multiplicative inverse of 9 in $\mathbb{Z}_{32}$ is 25; that is, $9^{-1} = 25$ in $\mathbb{Z}_{32}$.

We can check this as follows:

$$\begin{aligned} 25 \times 9 &= 225 \\ &= 7 \times 32 + 1, \end{aligned}$$

so $25 \times 9 \equiv 1 \pmod{32}$, as expected.

The next worked exercise gives another example of using this method to find a multiplicative inverse in a number system $\mathbb{Z}_n$. In this example the method is applied a little more efficiently.

Worked Exercise A41

Find the multiplicative inverse of 10 in $\mathbb{Z}_{27}$.

Solution

Apply Euclid's Algorithm to 27 and 10, stopping when the remainder 1 is obtained (since the final equation, with remainder 0, is not needed).

Applying Euclid's Algorithm gives

$$\begin{aligned} 27 &= 2 \times 10 + 7 \\ 10 &= 7 + 3 \\ 7 &= 2 \times 3 + 1. \end{aligned}$$

Apply backwards substitution – we can do so by mentally rearranging the equations above as we need them; the rearranged equations are $1 = 7 - 2 \times 3$, $3 = 10 - 7$ and $7 = 27 - 2 \times 10$.

Starting with the last equation, we have

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 2(10 - 7) \\ &= -2 \times 10 + 3 \times 7 \\ &= -2 \times 10 + 3(27 - 2 \times 10) \\ &= 3 \times 27 - 8 \times 10. \end{aligned}$$

This final equation expresses 1 in terms of multiples of 27 and 10, and can be rearranged as $(-8) \times 10 = (-3) \times 27 + 1$.

Hence

$$(-8) \times 10 \equiv 1 \pmod{27}.$$

But $-8 \equiv 19 \pmod{27}$, so

$$19 \times 10 \equiv 1 \pmod{27},$$

and hence

$$19 \times_{27} 10 = 1.$$

Therefore $10^{-1} = 19$ in $\mathbb{Z}_{27}$.

A check: $19 \times 10 = 190 = 7 \times 27 + 1$, so $19 \times 10 \equiv 1 \pmod{27}$.

Exercise A97

Find the multiplicative inverse of

(a) 7 in $\mathbb{Z}_{16}$; (b) 8 in $\mathbb{Z}_{51}$.

The method demonstrated above can be used to find a multiplicative inverse of an element a in a number system $\mathbb{Z}_n$ whenever a and n are coprime. (The condition that a and n are coprime ensures that when we carry out backwards substitution we have 1 on the left-hand side of the equation; this 1 then becomes the 1 in the congruence of the form $ab \equiv 1 \pmod{n}$.)

On the other hand, if a and n are *not* coprime, then a has no multiplicative inverse in $\mathbb{Z}_n$. To see this, suppose that a and n are not coprime. If a did have a multiplicative inverse, say b, in $\mathbb{Z}_n$, then we would have

$$ab \equiv 1 \pmod{n},$$

that is,

$$ab = kn + 1 \text{ for some integer } k.$$

But a and n, not being coprime, are both divisible by some integer greater than 1, and hence $ab - kn$ is also divisible by this integer, which is impossible, since $ab - kn = 1$ by the equation above.

So we have the following result.

Theorem A11

Let n and a be positive integers, with a in $\mathbb{Z}_n$.

- If a and n are coprime, then a has a multiplicative inverse in $\mathbb{Z}_n$.
- If a and n are not coprime, then a does not have a multiplicative inverse in $\mathbb{Z}_n$.

Note that a more concise version of Theorem A11 is given in Subsection 1.4 of Unit A3, and this is the version stated in the module Handbook.

Theorem A11 gives us a further important result in the case when the modulus n is a *prime number*.

Remember that a **prime number** (or **prime**) is an integer greater than 1 whose only positive factors are 1 and itself; the first few primes are 2, 3, 5, 7, 11, 13, 17, and 19. In contrast, a **composite number** is an integer greater than 1 that is not a prime number; the first few composite numbers are 4, 6, 8, 9, 10, 12, 14, 15.

A prime number is necessarily coprime to every non-zero integer that is not a multiple of itself, so if p is a prime number, then every non-zero element of $\mathbb{Z}_p$ is coprime to p. Thus, by Theorem A11, we have the following result.

Multiplicative inverses in $\mathbb{Z}_p$

Let p be a prime number. Then every non-zero element in $\mathbb{Z}_p$ has a multiplicative inverse in $\mathbb{Z}_p$.

It follows that for multiplication in $\mathbb{Z}_p$, where p is a prime, we can add the following property to the list of properties of multiplication in $\mathbb{Z}_n$.

M4 Multiplicative inverses For each non-zero $a \in \mathbb{Z}_p$ where p is a prime number, there is a number $a^{-1} \in \mathbb{Z}_p$ such that

$$a \times_p a^{-1} = 1 = a^{-1} \times_p a.$$

So arithmetic with $+_p$ and $\times_p$ in $\mathbb{Z}_p$, where p is a prime, satisfies all the properties A1–A5 and M1–M5; that is, for both addition and multiplication we have closure, associativity, an identity, inverses of all non-zero elements, and commutativity. Also, the distributive property (D1) holds for combining addition and multiplication. So, if p is a prime, then the number system $\mathbb{Z}_p$ with arithmetic modulo p satisfies all the properties in the list of eleven properties of $\mathbb{R}$ that you met in Subsection 1.2. It also satisfies the twelfth, trivial, property mentioned (since the additive identity 0 and multiplicative identity 1 of $\mathbb{Z}_p$ are not equal). Therefore, when p is a prime, the number system $\mathbb{Z}_p$ with arithmetic modulo p is a *field*, like $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$.

However, the multiplicative inverses property (M4) does not hold for $\mathbb{Z}_n$ if n is not prime, since in that case some elements $a \in \mathbb{Z}_n$ do not have multiplicative inverses. So in general the number system $\mathbb{Z}_n$ with arithmetic modulo n is *not* a field.

3.5 Solving linear equations in $\mathbb{Z}_n$

We now return to the question of whether we can find solutions of equations in modular arithmetic. We consider linear equations, that is, equations of the form

$$a \times_n x = b,$$

where $a, b \in \mathbb{Z}_n$. We seek all solutions $x \in \mathbb{Z}_n$.

Linear equations $a \times_n x = b$ where a and n are coprime

First we consider the case where a and n are coprime. In this case, by Theorem A11, a has a multiplicative inverse a^{-1}, and we can solve the linear equation above by multiplying both sides by this inverse. In the special case where n is a prime number, *every* element of $\mathbb{Z}_n$ has a multiplicative inverse, so every linear equation $a \times_n x = b$ has a solution.

Worked Exercise A42

Solve the equation $10 \times_{27} x = 14$.

Solution

In Worked Exercise A41 we found that the multiplicative inverse of 10 in $\mathbb{Z}_{27}$ is 19. Multiplying both sides of the given equation

$$10 \times_{27} x = 14$$

by this multiplicative inverse gives

$$10^{-1} \times_{27} 10 \times_{27} x = 10^{-1} \times_{27} 14,$$

that is,

$$1 \times_{27} x = 19 \times_{27} 14.$$

Since

$$19 \times 14 \equiv 266 \equiv 266 - 270 \equiv -4 \equiv 23 \pmod{27},$$

we have $x = 23$.

Hence the equation $10 \times_{27} x = 14$ has solution $x = 23$.

Note that the solution found in Worked Exercise A42 is the *only* solution of the given equation, because the multiplicative inverse of 10 in $\mathbb{Z}_{27}$ is unique.

In general, by an argument similar to that of Worked Exercise A42, if a and n are coprime, then the linear equation

$$a \times_n x = b$$

has the *unique* solution

$$x = a^{-1} \times_n b.$$

Exercise A98

Solve the following linear equations.

(a) $7 \times_{16} x = 3$ (b) $8 \times_{51} x = 19$

(By the solution to Exercise A97, we have $7^{-1} = 7$ in $\mathbb{Z}_{16}$, and $8^{-1} = 32$ in $\mathbb{Z}_{51}$.)

To use the method of Worked Exercise A42 to solve an equation $a \times_n x = b$ where a and n are coprime, we first need to find the multiplicative inverse in $\mathbb{Z}_n$ of the coefficient a of x. If we have not already found this inverse (for example, by using Euclid's Algorithm and backwards substitution), and the modulus n is fairly small, then the quickest way to solve the equation may be just to try different values of x. We know that there is a unique solution, so we can stop trying values once we have found a solution. Sometimes a solution can be spotted by using congruences, as in the following worked exercise.

Worked Exercise A43

Solve the equation $5 \times_{12} x = 7$.

Solution

Spotting a congruence for 7 (mod 12) that is a multiple of 5 can be helpful.

Observe that $7 \equiv -5 \pmod{12}$, and we know $5 \times (-1) = -5$, so we have

$$5 \times (-1) \equiv 7 \pmod{12}.$$

The integer -1 is not an element of $\mathbb{Z}_{12}$, but $-1 \equiv 11 \pmod{12}$, so

$$5 \times 11 \equiv 7 \pmod{12};$$

that is,

$$5 \times_{12} 11 = 7.$$

Hence the solution of the given equation is $x = 11$.

Exercise A99

Solve the following equations.

(a) $5 \times_{13} x = 2$ (b) $3 \times_{11} x = 5$

You may spot solutions using congruences as in Worked Exercise A43, or you may prefer to try values, or find and use multiplicative inverses.

Linear equations $a \times_n x = b$ where a and n are not coprime

Recall that we are considering the question of whether we can find solutions in $\mathbb{Z}_n$ of equations of the form

$$a \times_n x = b \tag{5}$$

where $a, b \in \mathbb{Z}_n$. You have seen how to solve an equation of this form when a and n are coprime, so we now consider the case where a and n are not coprime.

In this case, the equation may not have any solutions. To see this, observe that if equation (5) *does* have a solution, say c, then

$$a \times_n c = b,$$

so

$$ac = b + kn \text{ for some integer } k,$$

which gives

$$b = ac - kn.$$

This equation tells us that any integer that is a factor of both a and n must also be a factor of b. Therefore, if equation (5) *does not* satisfy this condition – that is, if there is an integer that is a factor of both a and n but not a factor of b – then the equation has no solutions. In particular, if the highest common factor (HCF) of a and n is not a factor of b, then the equation has no solutions.

For example, the equation

$$6 \times_{18} x = 4$$

has no solutions, because the HCF of 6 and 18 is 3, and 3 is not a factor of 4.

On the other hand, if the HCF of a and n *is* a factor of b, then it turns out that the equation always has a solution; in fact, it has d solutions, where d is the HCF.

The box below summarises these facts about when the equation has solutions, and it also specifies what the solutions are when they exist.

Linear equations in $\mathbb{Z}_n$

Let d be the highest common factor of the integers a and n in the equation

$$a \times_n x = b.$$

- If d is not a factor of b, then the equation has no solutions in $\mathbb{Z}_n$.

- If d is a factor of b, then the equation has d solutions in $\mathbb{Z}_n$. These solutions are given by

$$x = c, \quad x = c + \frac{n}{d}, \quad x = c + \frac{2n}{d}, \quad \dots, \quad x = c + \frac{(d-1)n}{d},$$

where c is the solution in $\mathbb{Z}_{n/d}$ of the simpler equation

$$\frac{a}{d} \times_{\frac{n}{d}} x = \frac{b}{d}.$$

(Since a/d and n/d are coprime, the simpler equation has a unique solution, which can be found using the methods given earlier.)

You will see a proof of the second bulleted statement in the box shortly. First, here is a worked exercise that illustrates the results in the box, and one similar exercise for you to try.

Worked Exercise A44

Solve the following equations.

(a) $4 \times_{12} x = 6$ (b) $6 \times_{15} x = 9$

Solution

(a) The HCF of 4 and 12 is 4, but this is not a factor of 6, so the equation $4 \times_{12} x = 6$ has no solutions.

(b) The HCF of 6 and 15 is $d = 3$, and this is also a factor of 9, so the equation $6 \times_{15} x = 9$ has $d = 3$ solutions.

To find these solutions, we start by finding the solution of the simpler equation

$$\frac{6}{3} \times_{\frac{15}{3}} x = \frac{9}{3},$$

that is,

$$2 \times_5 x = 3.$$

By trying possibilities, we find that the solution of this equation is

$$x = 4.$$

Also, $15/3 = 5$, so the solutions of the original equation are

$$x = 4, \quad x = 4 + 5 = 9, \quad x = x + 2 \times 5 = 14.$$

A quick check:

$$6 \times 4 = 24 \equiv 9 \pmod{15},$$
$$6 \times 9 = 54 \equiv 54 - 45 \equiv 9 \pmod{15},$$
$$6 \times 14 \equiv 6 \times (-1) \equiv -6 \equiv 9 \pmod{15},$$

as expected.

Exercise A100

Find all the solutions of the following equations.

(a) $9 \times_{12} x = 6$ (b) $8 \times_{12} x = 7$ (c) $5 \times_{12} x = 2$

(d) $4 \times_{16} x = 12$ (e) $3 \times_{16} x = 13$ (f) $8 \times_{16} x = 2$

As promised, here is a proof of the second bulleted statement in the box 'Linear equations in $\mathbb{Z}_n$'. Before reading it, look back to remind yourself what this statement says. To see why it holds, let c be the solution of the simpler equation, as stated. Then

$$\frac{a}{d} \times_{\frac{n}{d}} c = \frac{b}{d},$$

so

$$\frac{a}{d}c = \frac{b}{d} + k\frac{n}{d}$$

for some integer k, and hence (by multiplying throughout by d),

$$ac = b + kn,$$

so

$$a \times_n c = b,$$

that is, c is also a solution of the original equation.

Now consider all the integers r such that $c + r$ is in $\mathbb{Z}_n$ (where c is the solution discussed above). Let us consider the question: for which of these values of r is $c + r$ a solution of the original equation?

Well, saying that $c + r$ is a solution of the original equation is equivalent to saying that

$$a \times_n (c + r) = b,$$

which, by the multiplication property of congruences, is equivalent to saying that

$$a \times_n (c +_n r) = b.$$

By the distributive property for $+_n$ and $\times_n$, the equation above is equivalent to

$$(a \times_n c) +_n (a \times_n r) = b.$$

Now $a \times_n c = b$ (since c is a solution of the original equation), so the equation above is equivalent to

$$b +_n (a \times_n r) = b,$$

that is,

$$a \times_n r = 0.$$

So the values of r such that $c + r$ is a solution of the original equation are the values of r such that

ar is a multiple of n,

or, equivalently, since both a/d and n/d are integers,

$\dfrac{a}{d}r$ is a multiple of $\dfrac{n}{d}$.

Now we know that a/d is not a multiple of n/d, since these two integers are coprime, so the statement above holds precisely when r is a multiple of n/d. So our conclusion is that the element $c + r$ of $\mathbb{Z}_n$ is a solution of the original equation precisely when r is a multiple of n/d. This is what the second bulleted point in the box claims. (Note that the next multiple of n/d after $(d-1)n/d$ is $dn/d = n$, and adding n to c gives a number that is too large to be in $\mathbb{Z}_n$.)

Summary

In this unit you have studied the properties of various different number systems. You have seen that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_p$ (for p prime) all satisfy the eleven standard arithmetical properties you met in Subsection 1.2 (together with the trivial twelfth property) and so are all *fields*, and that the existence of a multiplicative inverse for every non-zero element means that every linear equation in these number systems has a solution. You also saw that in number systems that are not fields, for example, in $\mathbb{Z}$ and in $\mathbb{Z}_n$, where n is not prime, some, but certainly not all, linear equations have solutions. In the field $\mathbb{C}$, you saw that every *polynomial* equation with complex coefficients has a solution, and explored ways of finding such a solution in certain special cases.

These number systems and their properties are used throughout the rest of the module.

Learning outcomes

After working through this unit, you should be able to:

- understand the arithmetic properties of the rational and real numbers
- understand the properties a number system satisfies if it is a *field*
- understand and use the Factor Theorem
- understand the definition of a *complex number* and represent complex numbers as points in the *complex plane*
- perform arithmetic operations with complex numbers in *Cartesian*, *polar* and *exponential form*, and convert between these forms as appropriate
- use de Moivre's Theorem to find the nth roots of a complex number
- understand the Division Theorem and the properties of *congruences*, and perform *modular arithmetic*
- use Euclid's Algorithm and backwards substitution to find multiplicative inverses in modular arithmetic, where these exist
- solve linear equations in $\mathbb{Z}_n$.

Solutions to exercises

Solution to Exercise A57

(a) There is no integer 2^{-1} such that $2 \times 2^{-1} = 2^{-1} \times 2 = 1$, since $\frac{1}{2} \notin \mathbb{Z}$, for example.

(b) Only the numbers 1 and -1 have a multiplicative inverse in $\mathbb{Z}$. (The multiplicative inverse of 1 is 1, and of -1 is -1.)

Solution to Exercise A58

(a) **(i)** The equation has solution $x = -2$, which belongs to $\mathbb{Q}$.

(ii) The equation has solution $x = -\frac{1}{5}$, which belongs to $\mathbb{Q}$.

(b) **(i)** The equation has solution $x = 3$, which belongs to $\mathbb{R}$.

(ii) The equation has solution $x = -\dfrac{7}{\sqrt{3}}$, which belongs to $\mathbb{R}$.

Solution to Exercise A59

(a) Factorising the equation

$$x^2 - 7x + 12 = 0$$

gives

$$(x-3)(x-4) = 0.$$

So this equation has two solutions in $\mathbb{R}$, namely $x = 3$ and $x = 4$.

(b) Factorising the equation

$$x^2 + 6x + 9 = 0$$

gives

$$(x+3)^2 = 0.$$

So this equation has one solution in $\mathbb{R}$, namely $x = -3$.

(c) Factorising the equation

$$2x^2 + 5x - 3 = 0$$

gives

$$(2x-1)(x+3) = 0.$$

So this equation has two solutions in $\mathbb{R}$, namely $x = \frac{1}{2}$ and $x = -3$.

(d) Applying the quadratic formula to the equation

$$2x^2 - 2x - 1 = 0$$

gives

$$x = \frac{2 \pm \sqrt{4+8}}{4} = \frac{1}{2} \pm \frac{1}{2}\sqrt{3}.$$

This equation has two solutions in $\mathbb{R}$.

(e) Applying the quadratic formula to the equation

$$x^2 - 2x + 5 = 0$$

gives

$$x = \frac{2 \pm \sqrt{4-20}}{2}.$$

Since $4 - 20 = -16$, which is negative, this equation has no solutions in $\mathbb{R}$.

(f) Factorising the equation

$$x^2 - 2\sqrt{3}x + 3 = 0$$

gives

$$\left(x - \sqrt{3}\right)^2 = 0.$$

So this equation has one solution in $\mathbb{R}$, namely $x = \sqrt{3}$.

Solution to Exercise A60

(a) By the Factor Theorem (Theorem A2), $x + 3$ is a factor of $p(x)$ if and only if $p(-3) = 0$, that is,

$$\begin{aligned} 0 &= (-3)^3 + k(-3)^2 + 6(-3) + 36 \\ &= -27 + 9k - 18 + 36 \\ &= 9k - 9. \end{aligned}$$

This equation has just one solution, $k = 1$, so the only value of k for which $x + 3$ is a factor of $p(x)$ is $k = 1$.

(b) We have

$$x^3 + x^2 + 6x + 36 = (x+3)(ax^2 + bx + c),$$

for some real numbers a, b and c.

Equating the coefficients of x^3 gives $1 = a$. Comparing the constant terms gives $36 = 3c$, so $c = 12$. Thus we have

$$x^3 + x^2 + 6x + 36 = (x+3)(x^2 + bx + 12).$$

Equating the coefficients of x^2 gives $1 = 3 + b$, so $b = -2$. Hence

$$x^3 + x^2 + 6x + 36 = (x+3)(x^2 - 2x + 12).$$

Solution to Exercise A61

(a) Since all the roots are integers, the only possible roots are the factors of -15, that is, $\pm1, \pm3, \pm5, \pm15$. Considering these in turn, we obtain the following table.

x	1	-1	3	-3	5	$\cdots$
$p(x)$	0	-48	0	-192	0	$\cdots$

We do not need to work out any more values, as we already have three roots: $x = 1$, $x = 3$ and $x = 5$. So, since the coefficient of x^3 is 1,

$$p(x) = (x-1)(x-3)(x-5).$$

As a check, we note that the coefficient of x^2 is equal to minus the sum of the roots, $-9 = -(1+3+5)$.

(b) Let

$$p(x) = x^3 - 3x^2 + 4.$$

Since all the roots of $p(x)$ are integers, the only possible roots are the factors of 4, that is, $\pm1, \pm2, \pm4$. Considering these in turn, we obtain the following table.

x	1	-1	2	-2	4	-4
$p(x)$	2	0	0	-16	20	-108

Thus the only solutions are $x = -1$ and $x = 2$. Since $p(x)$ is a cubic polynomial, it must have three linear factors, so one of these solutions must give rise to a repeated factor. The coefficient of x^2 is -3, and this must equal minus the sum of the roots. This is only possible if $(x-2)$ is the repeated factor; we then have $-3 = -(2+2-1)$. The coefficient of x^3 is 1, so

$$p(x) = (x-2)(x-2)(x+1).$$

Solution to Exercise A62

(a) A suitable equation is

$$(x-1)(x-2)(x-3)(x+3) = 0,$$

that is,

$$x^4 - 3x^3 - 7x^2 + 27x - 18 = 0.$$

There are many other possibilities; for example, any of the factors could be repeated.

(b) A suitable equation is

$$(x-2)(x-2)(x-3) = 0,$$

that is,

$$x^3 - 7x^2 + 16x - 12 = 0.$$

Another possibility is

$$(x-2)(x-3)(x-3) = 0,$$

that is,

$$x^3 - 8x^2 + 21x - 18 = 0.$$

Solution to Exercise A63

(a) The equation $z^2 - 4z + 7 = 0$ has solutions

$$\begin{aligned} z = \frac{4 \pm \sqrt{16-28}}{2} &= \frac{4 \pm \sqrt{-12}}{2} \\ &= 2 \pm \frac{i\sqrt{12}}{2} \\ &= 2 \pm i\sqrt{3}; \end{aligned}$$

that is, the solutions are $z = 2 + i\sqrt{3}$ and $z = 2 - i\sqrt{3}$.

(b) The equation $z^2 - iz + 2 = 0$ has solutions

$$\begin{aligned} z = \frac{i \pm \sqrt{i^2 - 8}}{2} &= \frac{i}{2} \pm \frac{\sqrt{-9}}{2} \\ &= \frac{i}{2} \pm \frac{3i}{2}; \end{aligned}$$

that is, the solutions are $z = 2i$ and $z = -i$.

(c) We can factorise the equation

$$z^3 - 3z^2 + 4z - 2 = 0$$

as

$$(z-1)(az^2 + bz + c) = 0,$$

and by equating coefficients we have $a = 1$, $c = 2$ and $b = -2$ giving

$$(z-1)(z^2 - 2z + 2) = 0.$$

Hence $z = 1$ or

$$\begin{aligned} z &= \frac{2 \pm \sqrt{4-8}}{2} \\ &= \frac{2 \pm 2\sqrt{-1}}{2} \\ &= 1 \pm i, \end{aligned}$$

so the solutions are $z = 1$, $z = 1 + i$ and $z = 1 - i$.

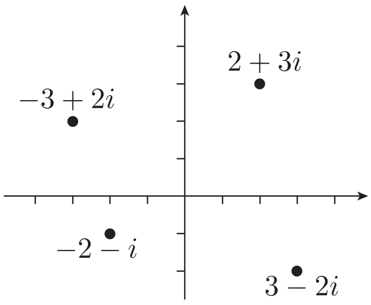
(d) The equation $z^4 - 16 = 0$ can be factorised as

$$(z^2 - 4)(z^2 + 4) = 0$$

giving $z^2 = 4$ or $z^2 = -4$, so $z = \pm 2$ or $z = \pm 2i$.

Hence the solutions are $z = 2$, $z = -2$, $z = 2i$ and $z = -2i$.

Solution to Exercise A64



Solution to Exercise A65

(a) $(3-5i) + (2+4i) = 5 - i$

(b) $$\begin{aligned}(2-3i)(-3+2i) &= -6 + 9i + 4i - 6i^2 \\ &= 13i\end{aligned}$$

(c) $$\begin{aligned}(5+3i)^2 &= (5+3i)(5+3i) \\ &= 25 + 15i + 15i + 9i^2 \\ &= 16 + 30i\end{aligned}$$

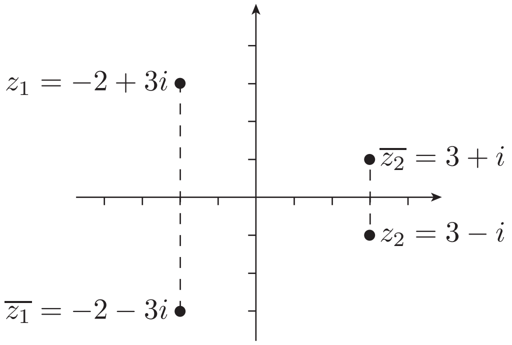
(d) $$\begin{aligned}(1+i)(7+2i) &= 7 + 7i + 2i + 2i^2 \\ &= 5 + 9i,\end{aligned}$$

so

$$\begin{aligned}(1+i)(7+2i)(4-i) &= (5+9i)(4-i) \\ &= 20 + 36i - 5i - 9i^2 \\ &= 29 + 31i.\end{aligned}$$

Solution to Exercise A66

$\overline{z_1} = -2 - 3i$ and $\overline{z_2} = 3 + i$.



Solution to Exercise A67

Property 2

Let $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$. Then

$$\begin{aligned} z_1 z_2 &= (x_1 + iy_1)(x_2 + iy_2) \\ &= x_1x_2 + ix_2y_1 + ix_1y_2 + i^2y_1y_2 \\ &= (x_1x_2 - y_1y_2) + i(x_2y_1 + x_1y_2), \end{aligned}$$

so

$$\overline{z_1 z_2} = (x_1x_2 - y_1y_2) - i(x_2y_1 + x_1y_2).$$

Also,

$$\begin{aligned} \overline{z_1} \times \overline{z_2} &= (x_1 - iy_1)(x_2 - iy_2) \\ &= x_1x_2 - ix_2y_1 - ix_1y_2 + i^2y_1y_2 \\ &= (x_1x_2 - y_1y_2) - i(x_2y_1 + x_1y_2). \end{aligned}$$

Therefore

$$\overline{z_1 z_2} = \overline{z_1} \times \overline{z_2}.$$

Property 3

Let $z = x + iy$. Then

$$\begin{aligned} z + \overline{z} &= x + iy + x - iy \\ &= 2x \\ &= 2\,\mathrm{Re}\,z. \end{aligned}$$

Property 4 Let $z = x + iy$. Then

$$\begin{aligned} z - \overline{z} &= x + iy - (x - iy) \\ &= 2iy \\ &= 2i \operatorname{Im} z. \end{aligned}$$

Solution to Exercise A68

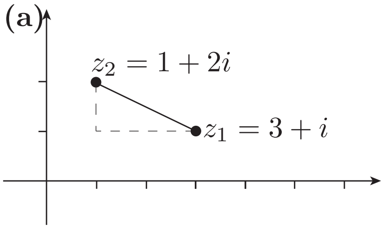
(a) $$\begin{aligned} |5 + 12i| &= \sqrt{5^2 + 12^2} \\ &= \sqrt{169} = 13 \end{aligned}$$

(b) $|1 + i| = \sqrt{1^2 + 1^2} = \sqrt{2}$

(c) $|-5| = \sqrt{(-5)^2 + 0^2} = 5$

Solution to Exercise A69

(a)



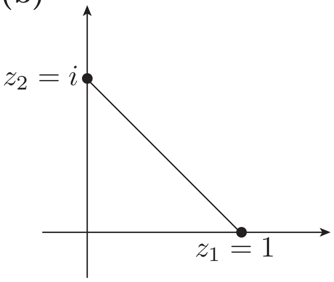
Here

$$z_1 - z_2 = (3 + i) - (1 + 2i) = 2 - i,$$

so

$$|z_1 - z_2| = \sqrt{2^2 + (-1)^2} = \sqrt{5}.$$

(b)



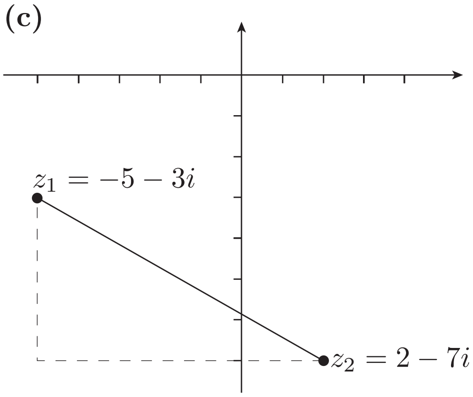
Here

$$z_1 - z_2 = 1 - i,$$

so

$$|z_1 - z_2| = \sqrt{1^2 + (-1)^2} = \sqrt{2}.$$

(c)



Here

$$z_1 - z_2 = (-5 - 3i) - (2 - 7i) = -7 + 4i,$$

so

$$|z_1 - z_2| = \sqrt{(-7)^2 + 4^2} = \sqrt{65}.$$

Solution to Exercise A70

In each case we multiply both the numerator and the denominator by the complex conjugate of the denominator, and use $z\overline{z} = |z|^2$.

(a) $$\begin{aligned} \frac{1}{3 - i} &= \frac{3 + i}{(3 - i)(3 + i)} \\ &= \frac{3 + i}{3^2 + (-1)^2} \\ &= \tfrac{3}{10} + \tfrac{1}{10}i \\ &= \tfrac{1}{10}(3 + i) \end{aligned}$$

(b) $$\begin{aligned} \frac{1}{-1 + 2i} &= \frac{-1 - 2i}{(-1 + 2i)(-1 - 2i)} \\ &= \frac{-1 - 2i}{(-1)^2 + 2^2} \\ &= -\tfrac{1}{5} - \tfrac{2}{5}i \\ &= -\tfrac{1}{5}(1 + 2i) \end{aligned}$$

Solution to Exercise A71

In each case we multiply the numerator and denominator by the complex conjugate of the denominator, and use $z\overline{z} = |z|^2$.

(a) $$\begin{aligned} \frac{5}{2 - i} &= \frac{5(2 + i)}{(2 - i)(2 + i)} \\ &= \frac{10 + 5i}{2^2 + (-1)^2} \\ &= \tfrac{1}{5}(10 + 5i) \\ &= 2 + i \end{aligned}$$

(b)
$$\begin{aligned}\frac{2+3i}{-3+4i} &= \frac{(2+3i)(-3-4i)}{(-3+4i)(-3-4i)}\\ &= \frac{-6-9i-8i-12i^2}{(-3)^2+4^2}\\ &= \frac{6-17i}{(-3)^2+4^2}\\ &= \tfrac{6}{25}-\tfrac{17}{25}i\\ &= \tfrac{1}{25}(6-17i)\end{aligned}$$

Solution to Exercise A72

(a) The required form is $x+iy$, where

$$x = 2\cos\frac{\pi}{2} = 0$$

and

$$y = 2\sin\frac{\pi}{2} = 2.$$

The Cartesian form is therefore $2i$.

(b) The required form is $x+iy$, where

$$\begin{aligned}x &= 4\cos\left(-\frac{2\pi}{3}\right) = 4\cos\frac{2\pi}{3}\\ &= -4\cos\frac{\pi}{3} = -2\end{aligned}$$

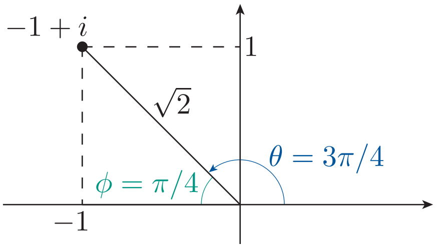
and

$$\begin{aligned}y &= 4\sin\left(-\frac{2\pi}{3}\right) = -4\sin\frac{2\pi}{3}\\ &= -4\sin\frac{\pi}{3} = -2\sqrt{3}.\end{aligned}$$

The Cartesian form is therefore $-2(1+i\sqrt{3})$.

Solution to Exercise A73

(a) Let $z = x+iy = -1+i$, so $x=-1$ and $y=1$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{(-1)^2+1^2} = \sqrt{2}.$$

Also

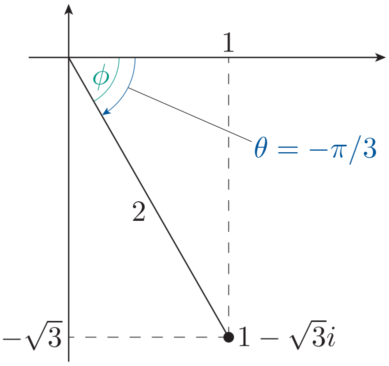
$$\cos\phi = \frac{|x|}{r} = \frac{1}{\sqrt{2}}.$$

So $\phi = \pi/4$, and from the diagram (or because z lies in the second quadrant) we have $\theta = \pi - \phi = 3\pi/4$.

Thus the polar form of $-1+i$ in terms of the principal argument is

$$\sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right).$$

(b) Let $z = x+iy = 1-i\sqrt{3}$, so $x=1$ and $y=-\sqrt{3}$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{1^2+(-\sqrt{3})^2} = 2.$$

Also

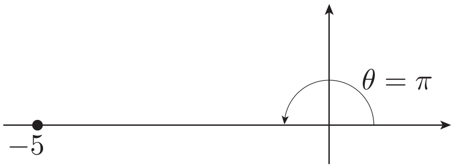
$$\cos\phi = \frac{|x|}{r} = \frac{1}{2}.$$

So $\phi = \pi/3$, and z lies in the fourth quadrant, so $\theta = -\phi = -\pi/3$.

Thus the polar form of $1-i\sqrt{3}$ in terms of the principal argument is

$$2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right).$$

(c) Let $z = x+iy = -5$, so $x=-5$ and $y=0$.



Then $z = r(\cos\theta + i\sin\theta)$, where

$$r = \sqrt{(-5)^2+0^2} = 5.$$

Also z lies on the negative half of the real axis, so $\theta = \pi$.

Thus the polar form of -5 in terms of the principal argument is

$$5(\cos\pi + i\sin\pi).$$

Solution to Exercise A74

(a) The modulus of the product is

$$4 \times \tfrac{1}{2} = 2.$$

An argument is

$$-\frac{\pi}{6} + \frac{7\pi}{8} = \frac{17\pi}{24}.$$

Since this argument lies in $(-\pi, \pi]$, it is the principal argument. The required product is therefore

$$2\left(\cos\frac{17\pi}{24} + i\sin\frac{17\pi}{24}\right).$$

The modulus of the quotient is

$$4 \div \tfrac{1}{2} = 8.$$

An argument is

$$-\frac{\pi}{6} - \frac{7\pi}{8} = -\frac{25\pi}{24}.$$

The principal argument is therefore

$$-\frac{25\pi}{24} + 2\pi = \frac{23\pi}{24}.$$

The required quotient is therefore

$$8\left(\cos\frac{23\pi}{24} + i\sin\frac{23\pi}{24}\right).$$

(b) The modulus of the product is

$$3 \times \tfrac{1}{2} = \tfrac{3}{2}.$$

An argument is

$$\frac{2\pi}{3} + \frac{\pi}{2} = \frac{7\pi}{6}.$$

The principal argument is therefore

$$\frac{7\pi}{6} - 2\pi = -\frac{5\pi}{6}.$$

The required product is therefore

$$\frac{3}{2}\left(\cos\left(-\frac{5\pi}{6}\right) + i\sin\left(-\frac{5\pi}{6}\right)\right).$$

The modulus of the quotient is

$$3 \div \tfrac{1}{2} = 6.$$

An argument is

$$\frac{2\pi}{3} - \frac{\pi}{2} = \frac{\pi}{6}.$$

Since this argument lies in $(-\pi, \pi]$, it is the principal argument. The required quotient is therefore

$$6\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right).$$

Solution to Exercise A75

From the solution to Exercise A73,

$$\begin{aligned}
z_1 &= \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right),\\
z_2 &= 2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right),\\
z_3 &= 5(\cos\pi + i\sin\pi).
\end{aligned}$$

Hence

$$\begin{aligned}
z_1z_2z_3 &= 10\sqrt{2}\left(\cos\left(\frac{3\pi}{4} - \frac{\pi}{3} + \pi\right)\right.\\
&\qquad\left. + i\sin\left(\frac{3\pi}{4} - \frac{\pi}{3} + \pi\right)\right)\\
&= 10\sqrt{2}\left(\cos\frac{17\pi}{12} + i\sin\frac{17\pi}{12}\right)\\
&= 10\sqrt{2}\left(\cos\left(-\frac{7\pi}{12}\right) + i\sin\left(-\frac{7\pi}{12}\right)\right),
\end{aligned}$$

using the principal argument.

Also

$$\begin{aligned}
\frac{z_2z_3}{z_1} &= \frac{10}{\sqrt{2}}\left(\cos\left(-\frac{\pi}{3} + \pi - \frac{3\pi}{4}\right)\right.\\
&\qquad\left. + i\sin\left(-\frac{\pi}{3} + \pi - \frac{3\pi}{4}\right)\right)\\
&= 5\sqrt{2}\left(\cos\left(-\frac{\pi}{12}\right) + i\sin\left(-\frac{\pi}{12}\right)\right).
\end{aligned}$$

Solution to Exercise A76

(a) $1 = \cos 0 + i \sin 0$

(b) If $z_0 = \cos 0 + i \sin 0$, then, by de Moivre's Theorem,

$$z_0^3 = \cos 0 + i \sin 0 = 1.$$

If $z_1 = \cos(2\pi/3) + i \sin(2\pi/3)$, then, by de Moivre's Theorem,

$$\begin{aligned} z_1^3 &= \cos 2\pi + i \sin 2\pi \\ &= \cos 0 + i \sin 0 = 1. \end{aligned}$$

If $z_2 = \cos(4\pi/3) + i \sin(4\pi/3)$, then, by de Moivre's Theorem,

$$\begin{aligned} z_2^3 &= \cos 4\pi + i \sin 4\pi \\ &= \cos 0 + i \sin 0 = 1. \end{aligned}$$

(c) In Cartesian form,

$$\begin{aligned} z_0 &= 1, \\ z_1 &= -\frac{1}{2}\left(1 - i\sqrt{3}\right), \\ z_2 &= -\frac{1}{2}\left(1 + i\sqrt{3}\right). \end{aligned}$$

Solution to Exercise A77

(a) Let $z = r(\cos\theta + i \sin\theta)$. Then, since

$$1 = 1(\cos 0 + i \sin 0),$$

we have

$$\begin{aligned} z^6 &= r^6(\cos 6\theta + i \sin 6\theta) \\ &= 1(\cos 0 + i \sin 0). \end{aligned}$$

Hence $r = 1^{1/6} = 1$ and $\theta = 0 + \dfrac{2k\pi}{6}$ for $k = 0, 1, \ldots, 5$, and the six solutions of $z^6 = 1$ are given by

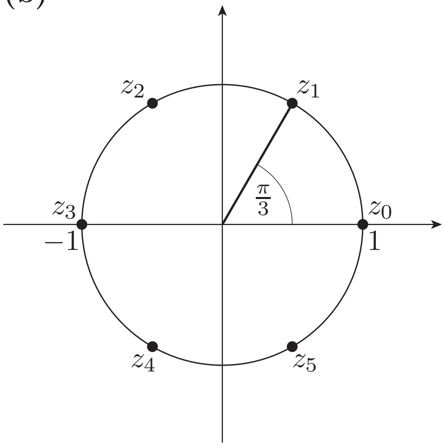
$$z = \cos\frac{2k\pi}{6} + i \sin\frac{2k\pi}{6}$$

for $k = 0, 1, \ldots, 5$.

Hence the solutions using the principal arguments are

$$\begin{aligned} z_0 &= \cos 0 + i \sin 0, \\ z_1 &= \cos\frac{\pi}{3} + i \sin\frac{\pi}{3}, \\ z_2 &= \cos\frac{2\pi}{3} + i \sin\frac{2\pi}{3}, \\ z_3 &= \cos\pi + i \sin\pi, \\ z_4 &= \cos\frac{4\pi}{3} + i \sin\frac{4\pi}{3} \\ &= \cos\left(-\frac{2\pi}{3}\right) + i \sin\left(-\frac{2\pi}{3}\right), \\ z_5 &= \cos\frac{5\pi}{3} + i \sin\frac{5\pi}{3} \\ &= \cos\left(-\frac{\pi}{3}\right) + i \sin\left(-\frac{\pi}{3}\right). \end{aligned}$$

(b)



(c)

$$\begin{aligned} z_0 &= 1, \\ z_1 &= \tfrac{1}{2}(1 + i\sqrt{3}), \\ z_2 &= -\tfrac{1}{2}(1 - i\sqrt{3}), \\ z_3 &= -1, \\ z_4 &= -\tfrac{1}{2}(1 + i\sqrt{3}), \\ z_5 &= \tfrac{1}{2}(1 - i\sqrt{3}). \end{aligned}$$

Solution to Exercise A78

Let $z = r(\cos\theta + i\sin\theta)$. Then, since

$$-4 = 4(\cos\pi + i\sin\pi),$$

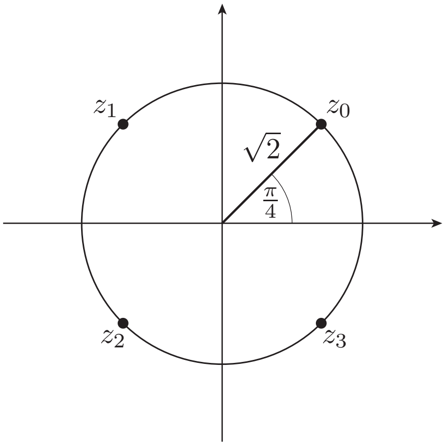
we have

$$z^4 = r^4(\cos 4\theta + i\sin 4\theta) = 4(\cos\pi + i\sin\pi).$$

Hence $r = 4^{1/4} = \sqrt{2}$ and $\theta = \dfrac{\pi}{4} + \dfrac{2k\pi}{4}$ for $k = 0, 1, 2, 3$.

So the solutions are

$$\begin{aligned} z_0 &= \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = 1 + i,\\ z_1 &= \sqrt{2}\left(\cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4}\right) = -1 + i,\\ z_2 &= \sqrt{2}\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = -1 - i,\\ z_3 &= \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right) = 1 - i. \end{aligned}$$



Solution to Exercise A79

Let $z = r(\cos\theta + i\sin\theta)$.

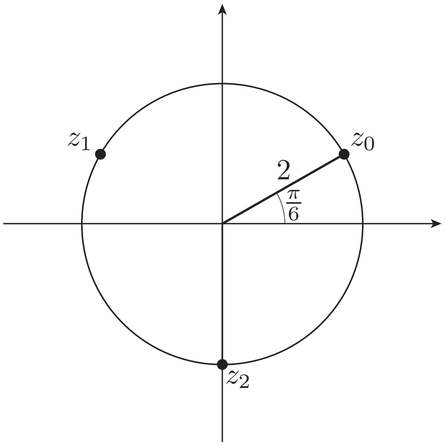
Since $8i = 8\left(\cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2}\right)$, we have

$$\begin{aligned} z^3 &= r^3(\cos 3\theta + i\sin 3\theta)\\ &= 8\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right). \end{aligned}$$

Hence $r = 8^{1/3} = 2$ and $\theta = \dfrac{\pi}{6} + \dfrac{2k\pi}{3}$ for $k = 0, 1, 2$.

So the solutions are

$$\begin{aligned} z_0 &= 2\left(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}\right) = \sqrt{3} + i,\\ z_1 &= 2\left(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}\right) = -\sqrt{3} + i,\\ z_2 &= 2\left(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}\right) = -2i. \end{aligned}$$



Solution to Exercise A80

(a) We have

$$\begin{aligned} p(2i) &= (2i)^4 - 2(2i)^3 + 7(2i)^2 - 8(2i) + 12\\ &= 16i^4 - 16i^3 + 28i^2 - 16i + 12\\ &= 16 + 16i - 28 - 16i + 12\\ &= 0, \end{aligned}$$

so $2i$ is a root of $p(z)$.

(b) Since p has real coefficients, $z = -2i$ is also a root of $p(z)$, so $(z - 2i)(z + 2i) = z^2 + 4$ is a factor of $p(z)$.

By equating coefficients, we obtain $z^4 - 2z^3 + 7z^2 - 8z + 12 = (z^2 + 4)(z^2 - 2z + 3)$.

So the remaining two roots of $p(z)$ are the solutions of the equation $z^2 - 2z + 3 = 0$.

Using the quadratic formula, we have

$$\begin{aligned} z &= \frac{2 \pm \sqrt{4 - 12}}{2}\\ &= \frac{2 \pm \sqrt{-8}}{2}\\ &= \frac{2 \pm 2\sqrt{-2}}{2}\\ &= 1 \pm i\sqrt{2}. \end{aligned}$$

Hence the four roots of $p(z)$ are $2i$, $-2i$, $1+i\sqrt{2}$ and $1-i\sqrt{2}$.

Solution to Exercise A81

A suitable polynomial is

$$(z-1)(z+2)(z-3i)(z+3i),$$

that is,

$$(z^2+z-2)(z^2+9)$$

or

$$z^4+z^3+7z^2+9z-18.$$

Solution to Exercise A82

(a) Let $z=x+iy$; then

$$\begin{aligned}\frac{1}{e^z}&=\frac{1}{e^{x+iy}}\\&=\frac{1}{e^x(\cos y+i\sin y)}\quad\text{(by definition)}\\&=e^{-x}(\cos y+i\sin y)^{-1}\\&=e^{-x}(\cos(-y)+i\sin(-y))\end{aligned}$$

(by de Moivre's Theorem with $n=-1$)

$$\begin{aligned}&=e^{-x+i(-y)}\quad\text{(by definition)}\\&=e^{-z}.\end{aligned}$$

(b) $$\begin{aligned}\frac{e^{z_1}}{e^{z_2}}&=e^{z_1}\times\frac{1}{e^{z_2}}\\&=e^{z_1}e^{-z_2}\quad\text{(by part (a))}\\&=e^{z_1+(-z_2)}\quad\text{(by Worked Exercise A36)}\\&=e^{z_1-z_2}.\end{aligned}$$

Solution to Exercise A83

Euler's Identity is $e^{i\pi}+1=0$; that is, $-1=e^{i\pi}$.

We have

$$\begin{aligned}-z&=-1\times re^{i\theta}\\&=e^{i\pi}\times re^{i\theta}\quad\text{(by Euler's Identity)}\\&=re^{i(\theta+\pi)}.\end{aligned}$$

Solution to Exercise A84

(a) $65=9\times 7+2$, so the quotient is 9 and the remainder is 2.

(b) $-256=-20\times 13+4$, so the quotient is -20 and the remainder is 4.

Solution to Exercise A85

(a) The possible remainders are 0, 1, 2, 3, 4, 5 and 6.

(b) There are many possible answers here; for example, 3, 10, -4 and -11.

Solution to Exercise A86

We have

$$\begin{aligned}25&\equiv 8 \pmod{17},\\53&\equiv 2 \pmod{17},\\-15&\equiv 2 \pmod{17},\\3&\equiv 3 \pmod{17},\\127&\equiv 8 \pmod{17},\end{aligned}$$

so the remainders are 8, 2, 2, 3 and 8, respectively. So $25\equiv 127 \pmod{17}$ and $53\equiv -15 \pmod{17}$.

Solution to Exercise A87

Suppose that $a\equiv b \pmod{n}$ and $c\equiv d \pmod{n}$. Then $a-b=kn$ and $c-d=ln$ for some integers k and l. Hence $a=b+kn$ and $c=d+ln$ for some integers k and l, so

$$\begin{aligned}ac&=(b+kn)(d+ln)\\&=bd+bln+knd+kln^2\\&=bd+n(bl+kd+kln).\end{aligned}$$

Therefore $ac-bd=(bl+kd+kln)n$. Since $bl+kd+kln$ is an integer, it follows that $ac\equiv bd \pmod{n}$. Thus the multiplication property holds.

Solution to Exercise A88

(a) Using the transitivity property of congruences we obtain

$$3869\equiv 669\equiv 29\equiv 13 \pmod{16}$$

and

$$1685\equiv 85\equiv 5 \pmod{16},$$

so 3869 has remainder 13 on division by 16, and 1685 has remainder 5 on division by 16.

(b) Using the addition property of congruences and the answer to part (a), we obtain

$$(3869 + 1685) \equiv (13 + 5) \equiv 18 \equiv 2 \pmod{16},$$

so $3869 + 1685$ has remainder 2 on division by 16.

(c) Using the powers property of congruences and the answer to part (b), we obtain

$$(3869 + 1685)^4 \equiv 2^4 \equiv 16 \equiv 0 \pmod{16},$$

so $(3869 + 1685)^4$ has remainder 0 on division by 16; that is, $(3869 + 1685)^4$ is divisible by 16.

Since

$$\begin{aligned}&(3869 + 1685)^{111}\\ &\quad = (3869 + 1685)^4 \times (3869 + 1685)^{107},\end{aligned}$$

the multiplication property of congruences gives

$$\begin{aligned}(3869 + 1685)^{111} &\equiv 0 \times (3869 + 1685)^{107}\\ &\equiv 0 \pmod{16}.\end{aligned}$$

Hence $(3869 + 1685)^{111}$ has remainder 0 on division by 16; that is, it is divisible by 16.

Alternatively, it is possible to conclude directly that $(3869 + 1685)^{111}$ is divisible by 16 (and hence has remainder 0 on division by 16) since it is divisible by $(3869 + 1685)^4$.

Solution to Exercise A89

(a) $3 +_5 2 = 0$

(b) $4 +_{17} 5 = 9$

(c) $8 +_{16} 12 = 4$

(d) $3 \times_5 2 = 1$

(e) $4 \times_{17} 5 = 3$

(f) $8 \times_{16} 12 = 0$

Solution to Exercise A90

There are many ways to calculate these products in modular arithmetic; your method may differ from those below.

(a) We have

$$\begin{aligned}7 \times 26 &\equiv 7 \times (-1)\\ &\equiv -7\\ &\equiv 20 \pmod{27}.\end{aligned}$$

Thus $7 \times_{27} 26 = 20$.

(b) We have

$$\begin{aligned}16 \times 14 &\equiv 8 \times 2 \times 14\\ &\equiv 8 \times 28\\ &\equiv 8 \times (-1)\\ &\equiv -8\\ &\equiv 21 \pmod{29}.\end{aligned}$$

Thus $16 \times_{29} 14 = 21$.

(c) We have

$$\begin{aligned}9 \times 15 &\equiv 3 \times 3 \times 15\\ &\equiv 3 \times 45\\ &\equiv 3 \times 12\\ &\equiv 36\\ &\equiv 3 \pmod{33}.\end{aligned}$$

Thus $9 \times_{33} 15 = 3$.

(d) We have

$$\begin{aligned}37 \times 23 &\equiv -8 \times 23\\ &\equiv -4 \times 2 \times 23\\ &\equiv -4 \times 46\\ &\equiv -4 \times 1\\ &\equiv -4\\ &\equiv 41 \pmod{45}.\end{aligned}$$

Thus $37 \times_{45} 23 = 41$.

(e) We have

$$\begin{aligned}15 \times 6 &\equiv 15 \times 2 \times 3\\ &\equiv 30 \times 3\\ &\equiv -4 \times 3\\ &\equiv -12\\ &\equiv 22 \pmod{34}.\end{aligned}$$

Thus $15 \times_{34} 6 = 22$.

(f) We have

$$\begin{aligned}9 \times 18 &\equiv 9 \times 9 \times 2\\ &\equiv 81 \times 2\\ &\equiv 1 \times 2\\ &\equiv 2 \pmod{40}.\end{aligned}$$

Thus $9 \times_{40} 18 = 2$.

Solution to Exercise A91

(a) From the tables, we have the following.

(i) $3 +_4 3 = 2$, so if $x +_4 3 = 2$ then $x = 3$.

(ii) $4 +_7 5 = 2$, so if $x +_7 5 = 2$ then $x = 4$.

(iii) $2 +_4 2 = 0$, so if $x +_4 2 = 0$ then $x = 2$.

(iv) $2 +_7 5 = 0$, so if $x +_7 5 = 0$ then $x = 2$.

(b) You may have noticed that:

- each element appears exactly once in each row and exactly once in each column
- there is a pattern of diagonal stripes of unique numbers running down from right to left.

Solution to Exercise A92

(a)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) $x +_6 1 = 5$ has solution $x = 4$.

$x +_6 5 = 1$ has solution $x = 2$.

Solution to Exercise A93

By definition, $a +_n b$ and $b +_n a$ are the remainders of the integers $a + b$ and $b + a$, respectively, on division by n. Since ordinary addition is commutative, we have $a + b = b + a$, so $a +_n b = b +_n a$, and the commutative property (A5) holds.

Solution to Exercise A94

(a)

a	0	1	2	3	4	5	6
$-_7 a$	0	6	5	4	3	2	1

(b)

a	0	1	2	$\dots$	r	$\dots$	$n-1$
$-_n a$	0	$n-1$	$n-2$	$\dots$	$n-r$	$\dots$	1

The additive inverse of 0 is always 0, since $0 +_n 0 = 0$.

For any integer $r > 0$ in $\mathbb{Z}_n$, $n - r \in \mathbb{Z}_n$ and $r + (n - r) = n$, so $r +_n (n - r) = 0$.

Solution to Exercise A95

(a) **(i)** The elements 1 and 3 of $\mathbb{Z}_4$ have multiplicative inverses in $\mathbb{Z}_4$: 1 has multiplicative inverse 1 since $1 \times_4 1 = 1$, and similarly 3 has multiplicative inverse 3 since $3 \times_4 3 = 1$. The other elements of $\mathbb{Z}_4$, namely 0 and 2, do not have multiplicative inverses.

(ii) The non-zero elements of $\mathbb{Z}_7$ have multiplicative inverses as given in the following table, where b is a multiplicative inverse of a.

a	1	2	3	4	5	6
b	1	4	5	2	3	6

(b)

$\times_{10}$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

The elements 1, 3, 7 and 9 of $\mathbb{Z}_{10}$ have multiplicative inverses in $\mathbb{Z}_{10}$, as given in the following table, where b is a multiplicative inverse of a.

a	1	3	7	9
b	1	7	3	9

The other elements of $\mathbb{Z}_{10}$, namely 0, 2, 4, 5, 6 and 8, do not have multiplicative inverses.

Solution to Exercise A96

Applying Euclid's Algorithm gives

$$
\begin{aligned}
201 &= 2 \times 81 + 39 \\
81 &= 2 \times 39 + 3 \\
39 &= 13 \times 3 + 0.
\end{aligned}
$$

The HCF of 201 and 81 is therefore 3. It follows that 201 and 81 are not coprime, and hence that 81 does not have a multiplicative inverse in $\mathbb{Z}_{201}$.

Solution to Exercise A97

(a) Euclid's Algorithm gives

$$\begin{aligned}16 &= 2\times 7+2\\ 7 &= 3\times 2+1.\end{aligned}$$

Starting with the last equation, we have

$$\begin{aligned}1 &= 7-3\times 2\\ &= 7-3(16-2\times 7)\\ &= -3\times 16+7\times 7.\end{aligned}$$

Hence $7\times 7 = 3\times 16+1$, so $7\times_{16} 7 = 1$ and therefore $7^{-1} = 7$ in $\mathbb{Z}_{16}$.

(b) Euclid's Algorithm gives

$$\begin{aligned}51 &= 6\times 8+3\\ 8 &= 2\times 3+2\\ 3 &= 1\times 2+1.\end{aligned}$$

Starting with the last equation, we have

$$\begin{aligned}1 &= 3-2\\ &= 3-(8-2\times 3)\\ &= -8+3\times 3\\ &= -8+3(51-6\times 8)\\ &= 3\times 51-19\times 8.\end{aligned}$$

Hence $(-19)\times 8\equiv 1 \pmod{51}$, but $-19+51=32$ so

$$32\times 8\equiv 1 \pmod{51}.$$

Hence $32\times_{51} 8 = 1$, so $8^{-1} = 32$ in $\mathbb{Z}_{51}$.

Solution to Exercise A98

(a) The given equation is

$$7\times_{16} x = 3.$$

Multiplying both sides by the multiplicative inverse of 7 in $\mathbb{Z}_{16}$, which is 7, gives

$$7\times_{16} 7\times_{16} x = 7\times_{16} 3$$

that is,

$$1\times_{16} x = x = 7\times_{16} 3.$$

Since $7\times 3 = 21 = 16+5$, we have $x=5$.

Thus the equation $7\times_{16} x = 3$ has solution $x=5$.

(b) The given equation is

$$8\times_{51} x = 19.$$

Multiplying both sides by the multiplicative inverse of 8 in $\mathbb{Z}_{51}$, which is 32, gives

$$32\times_{51} 8\times_{51} x = 32\times_{51} 19,$$

that is,

$$1\times_{51} x = x = 32\times_{51} 19.$$

Since $32\times 19 = 608 = 510+98 = 510+51+47$, we have $x=47$.

Thus the equation $8\times_{51} x = 19$ has solution $x=47$.

Solution to Exercise A99

(a) Observe that $2\equiv 15 \pmod{13}$, and we know $5\times 3 = 15$ so we have

$$5\times 3\equiv 2 \pmod{13}.$$

Hence the solution of the given equation is $x=3$.

Alternatively, $5^{-1} = 8$ in $\mathbb{Z}_{13}$ (since $5\times 8 = 40 = 39+1$, so $5\times_{13} 8 = 1$). We have $8\times 2 = 16 = 13+3$, so $x = 8\times_{13} 2 = 3$.

(b) Observe that $5\equiv -6 \pmod{11}$, and we know $3\times(-2) = -6$ so we have

$$3\times(-2)\equiv 5 \pmod{11}.$$

The integer -2 is not an element of $\mathbb{Z}_{11}$, but $-2\equiv 9 \pmod{11}$.

Hence the solution of the given equation is $x=9$.

Alternatively, $3^{-1} = 4$ in $\mathbb{Z}_{11}$ (since $3\times 4 = 12 = 11+1$, so $3\times_{11} 4 = 1$). We have $4\times 5 = 20 = 11+9$, so $x = 4\times_{11} 5 = 9$.

Solution to Exercise A100

(a) The HCF of 9 and 12 is $d = 3$, and this is also a factor of 6, so the equation $9 \times_{12} x = 6$ has $d = 3$ solutions.

To find the smallest solution of the given equation, we solve the equation

$$\frac{9}{3} \times_{\frac{12}{3}} x = \frac{6}{3},$$

that is,

$$3 \times_4 x = 2.$$

By trying possibilities, we find that this equation has solution $x = 2$, since $3 \times 2 = 6$ and $6 \equiv 2 \pmod 4$. Also $n/d = 12/3 = 4$, so the other solutions are $x = 2 + 4 = 6$ and $x = 2 + 2 \times 4 = 10$.

(b) The HCF of 8 and 12 is 4, but this is not a factor of 7, so the equation $8 \times_{12} x = 7$ has no solutions.

(c) The HCF of 5 and 12 is 1; that is, they are coprime. Hence the equation $5 \times_{12} x = 2$ has a unique solution.

The solution, $x = 10$, can be found in various ways: for example

- by noticing that $5 \times 5 = 25$ and $25 \equiv 1 \pmod{12}$, so $5^{-1} = 5$ in $\mathbb{Z}_{12}$ and therefore $x = 5^{-1} \times_{12} 2 = 10$
- by spotting that $2 \equiv -10 \pmod{12}$, so $5 \times (-2) \equiv 2 \pmod{12}$, and since $-2 \equiv 10 \pmod{12}$ we have $5 \times_{12} 10 = 2$
- by testing possible values for x.

(d) The HCF of 4 and 16 is $d = 4$, and this is also a factor of 12, so the equation $4 \times_{16} x = 12$ has $d = 4$ solutions.

To find the smallest solution of the given equation, we solve the equation

$$\frac{4}{4} \times_{\frac{16}{4}} x = \frac{12}{4},$$

that is,

$$1 \times_4 x = 3,$$

which simplifies to the solution $x = 3$.

Also $n/d = 12/3 = 4$, so the other solutions are $x = 3 + 4 = 7$, $x = 3 + 2 \times 4 = 11$ and $x = 3 + 3 \times 4 = 15$.

(e) The HCF of 3 and 16 is 1; that is, they are coprime. Hence the equation $3 \times_{16} x = 13$ has a unique solution.

The solution, $x = 15$, can be found in various ways. For example, you could test possible values for x: you would eventually find that

$$3 \times 15 = 45 = 2 \times 16 + 13$$

so $3 \times_{16} 15 = 13$. Alternatively, you might spot that $13 \equiv -3 \pmod{16}$, so

$$3 \times (-1) \equiv 13 \pmod{16}$$

which gives

$$3 \times 15 \equiv 13 \pmod{16},$$

and hence $3 \times_{16} 15 = 13$. Alternatively again, you might start by finding the multiplicative inverse of 3 in $\mathbb{Z}_{16}$; a quick way to do this is to observe that $3 \times 11 = 33 \equiv 1 \pmod{16}$, so $3^{-1} = 11$ in $\mathbb{Z}_{16}$. This gives $x = 3^{-1} \times_{16} 13 = 15$.

(f) The HCF of 8 and 16 is 8, but this is not a factor of 2, so the equation $8 \times_{16} x = 2$ has no solutions.